The High Technology Crime Advisory Committee

ANNUAL REPORT ON HIGH TECHNOLOGY CRIME IN CALIFORNIA

HIGH TECHNOLOGY CRIME IN CALIFORNIA

Table of Contents

1.0 EXECUTIVE SUMMARY

High technology crime presents a 21st Century challenge to the state of California as well as to the entire world. It is different from traditional types of crime. Traditional crime is local and easily understood; high technology crime is multi-jurisdictional, complex and beyond the expertise and resources of many small California police departments. Further, nearly every crime committed today has a high technology aspect - usually a personal computer which may hold evidence about the crime or its perpetrators.

In California high technology crime has been expanded to include crimes against manufacturers of computers, components and chips, and developers of software products. As defined in SB 1734 it includes:

- White-collar crime
- Computer and network crime
- Money laundering
- Telecommunications and cable television services crime
- Software piracy
- Theft and resale of computer components and other high tech products
- Remarking and counterfeiting of computer hardware and software
- Intellectual property and trade secrets theft

Every interview conducted for this report[1] and virtually every source of information uncovered on the subject indicates that high technology crime is growing rapidly. Even though there is currently a lack of statistical data on high technology crime, this study attempts to estimates its impacts in California. As described in Section 5.0, the estimated annual impacts are:

- Revenue Lost: $6,564 million
- Jobs Lost: 19,140
- Wages Lost: $923 million
- Tax Revenue Lost: $358 million

There are many victims of high technology crime: the public, high tech corporations, other corporations, utilities and the government. Fraud, illegal access to computers and networks, and the theft of computers affect virtually all segments of society. Chip and component theft affect hardware companies; piracy and remarking software affects the software and entertainment

[1] This report was prepared by Burke Information Technology Services, San Francisco, under a contract with the California Office of Criminal Justice Planning.

industries, and telecommunications and cable / satellite companies are affected by the theft of communications signals.

Strategy and Recommendations

The legislation that created the High Technology Theft Apprehension and Prosecution program and the High Technology Crime Advisory Committee (HTCAC) requires the development of a strategy to fight high technology crime. This strategy, the High Technology Theft Apprehension and Prosecution Strategy, is described in Section 7.0. The following recommendations are based on the strategy.

Expand the Task Force Approach based on Advisory Committees

The HTCAC strongly recommends that the task force approach to fighting high technology crime be expanded into new regions of California. Each task force will identify the most serious systemic high technology crime(s) in its region. Advisory Committees, including local high technology industries and other organizations, will assist each task force to assess crime risk and to prioritize high technology crime targets in the region.

Implement Data Collection and Database Development

The HTCAC strongly recommends that high technology crime data be collected by the task forces and that high tech crime database become available to the police forces and district attorneys of California as soon as possible. Each task force will be required to collect and maintain certain types of information on a common basis for inclusion in the database developed in cooperation with the California Department of Justice (DOJ) as part of the legislative mandate. The unwillingness of victims to report losses has led the public to underestimate the impact of high technology crime and has made it difficult for law enforcement agencies to determine which crimes are most serious.

Implement Training

The HTCAC recommends a statewide training program for high tech investigations and prosecution. This approach will insure that task force members receive training that is presented consistently throughout the state, and is updated annually in order to teach the latest trends in high technology crimes. Training should be provided in different regions of the state.

2.0 BACKGROUND

The approach to fight high technology crime in California has evolved over the last few years. The State of California's official role became official only within the last year with the passage of SB 1734[2].

Regional High Technology Crime Task Forces

California has been fighting high technology crime since the early 1990s when the theft of computer parts began to grow at an alarming rate.[3] The local response to this threat was the formation of a task force based on the informal relationships between cooperating police forces. The task force approach is particularly effective since high technology crime is usually cross-jurisdictional and requires joint and supporting approaches between jurisdictions, often between federal and local police agencies. Its resource requirements may be extensive and sophisticated and are often beyond the resources of local small or medium-sized police departments.

The development of task forces was recommended by the California High-Tech Task Force Committee as the approach to fight high technology crime[4]. Other police forces around the country have also concluded that the task force approach is the best way to fight high technology crime.[5] The State's role in the coordination and support of the high technology crime task forces is an extension of existing relationships with local, state and federal agencies.

In 1998, the State endorsed and further supported the task force approach with the passage of SB 1734, High Tech Crimes. As mandated in the law, task force programs and resources will be augmented by grants, to be administered by the Office of Criminal Justice Planning (OCJP), thus defining the role of the State in the fight against high technology crime.

California currently has three high technology task forces

- Los Angeles County and Orange County Regional High Tech Crime Task Force
- Rapid Enforcement Allied Computer Team (REACT), Silicon Valley
- Sacramento Valley Hi-Tech Crimes Task Force

[2] An act to amend Sections 502.01, 13848, 13848.2, 13848.4, and 13848.6 of the Penal Code, relating to computer crimes.
[3] See Eyres, 1999
[4] Ohlhausen, 1997
[5] Meyer, 1998

Participation in the High Technology Theft Apprehension and Prosecution Program will require the High Technology Crime Task Forces to collect and submit data to the State on an annual basis. This is a beginning of a programmatic effort to collect the required information. But more is needed - information about high technology crime should become part of the routine data collected about every crime. But in order for this to happen there will need to be agreement among national, state and local law enforcement organizations on the types and definitions of high technology crime.

The Role of the High Technology Crime Advisory Committee

The High Technology Crime Advisory Committee was established by SB 1734 to advise OCJP regarding high technology crime and assist it in the oversight of the regional task forces. SB 1734 also established the High Technology Crime Advisory Committee with a membership representing 15 organizations:

- American Electronic Association to represent California computer system manufacturers
- American Electronic Association to represent California computer software producers
- California Attorney General
- California Cable Television Association
- California Cellular Carriers Association
- California District Attorneys Association
- California Highway Patrol
- California Internet Industry Alliance
- California Office of Criminal Justice Planning
- California Police Chiefs Association
- California State Sheriffs Association
- California Telephone Association or the California Association of Long Distance Companies, rotating every other year between the two associations
- High Tech Criminal Investigators Association
- Motion Picture Association of America
- Semiconductor Equipment and Materials International

The committee will also assist OCJP to coordinate the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program and implemented by the regional task forces. Each of these task forces will identify systemic high technology crime in its region, will gather and analyze information to determine the key individuals responsible for the maintenance of the high technology crime system both within and outside of the region, and will use the gathered intelligence to build and prosecute cases against those individuals in conjunction with other agencies, including state and federal agencies.

The committee will also review the effectiveness of the regional task forces and provide its findings in a report to the Legislature and the Governor on an annual basis. This report shall be based on information provided by the regional task forces:

- The number of high technology crime cases filed in the prior year.
- The number of high technology crime cases investigated in the prior year.
- The number of victims involved in the cases filed.
- The number of convictions obtained in the prior year.
- The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

Interviews of High Technology Crime Organizations

This report is based on interviews with over 60 representatives of California public and private organizations interested in stopping high technology crime. Many of these organizations were associated with the three existing high technology crime task forces in the State. Comments from these interviews appear throughout the report in boxes, such as the one below. The organizations are listed in Appendix A.

> *Comments from interviews with high technology crime experts appear in boxes such as this one.*

The Following Sections

The sections that follow introduce the reader to key points about high technology crime, describe the types and levels of crime, as well as its impacts. The experience of the regional high technology crime task forces is described and a strategy to guide the fight against high technology crime is presented. Finally, the High Technology Crime Database is described and conclusions are drawn. These sections are:

3.0 An Introduction to High Technology Crime
4.0 Types and Costs of High Technology Crime
5.0 Impacts Of High Technology Crime
6.0 The Regional Task Force Experience
7.0 High Technology Theft Apprehension and Prosecution Strategy
8.0 The High Technology Crime Database System
9.0 Conclusions

3.0 AN INTRODUCTION TO HIGH TECHNOLOGY CRIME

Law enforcement officials in California are facing new types of crime that require new approaches and new types of resources. Known as high technology crime, computer crime or computer-related crime, this type of crime is increasing with the growth of the Internet, especially the World Wide Web (WWW)[6], and with the growth the high tech economy[7].

Not suprisingly, the adoption of the Internet for business and personal transactions[8] is beginning to attract an increasing level of criminal activity. The number of potential victims is growing, along with the number of potential perpetrators who have access to a computer and the Internet. Translated into future crimes, this growth threatens to overwhelm the resources of local law enforcement and district attorneys' offices throughout California.

> *Tracking high tech crimes is more labor intensive and time consuming than traditional crimes.*

> *We are implementing systems faster than we can secure them. And we have no institutional memory. Earlier mistakes keep coming back to haunt us.*

Definitions of High Technology Crime

Law enforcement officials don't always agree about what constitutes high technology crime. In part, this is due to the emphasis brought about by local conditions or organizational priorities. Different local areas have different types of high technology crime. Crime affecting the "high tech" industry in California, the theft and remarking of chips, components and computers, is

[6] The "Web" consists of about 800 million pages on the publicly indexable World Wide Web, residing on approximately 3 million servers and growing at the rate of approximately 14 million pages per month, down from approximately 45 million pages a month in December 1998. (Lawrence and Giles, 1998, 1999)

[7] As reported in AEA's Cyberstates 3.0 (1999), California had over 784,000 high-tech jobs in 1997, with a payroll of $49.2 billion, that is increasing at 9% or 66,100 jobs per year. 61% of all exports from California are the products and services of high technology industries such as software services, communications services, computers and office equipment manufacturing, electronics components and accessories manufacturing and semiconductor manufacturing.

[8] A recent study by the University of Texas, The Internet Economy Indicators, pegged 1998 E-Commerce revenues at $301 billion in 1998 (supporting an estimated 1.2 million jobs), up from approximately $5 billion in 1995. The International Data Corporation projects that E-commerce revenues will reach $1 trillion by 2003. To support sales growth, businesses will invest $23.6 billion by 2002 to upgrade their electronic commerce systems, according to ActivMedia.

important because of economic losses that occur when these items are sold through the "gray market".

The California Legislature has defined high technology crime to be:

> *"Those crimes in which technology is used as an instrument in committing, or assisting in the commission of a crime, or which is the target of a criminal act."* [9]

Others define these sorts of crimes more narrowly such as a computer crime, or cybercrime, which is defined to be a crime in which the perpetrator uses special knowledge about computer technology.[10]

> *High tech crime needs to be adequately and precisely defined. Law enforcement often will require considerable evaluation and discussion to determine if a specific crime is, in fact, a high tech crime.*

In California high technology crime has been expanded to include crimes against manufacturers of computers, components and chips, and developers of software products.

These types of crimes in California are defined in SB 1734 to include but are not limited to:

- White-collar crime
- Computers and networks crime
- Money laundering
- Telecommunications and cable television services crime
- Software piracy
- Theft and resale of computer components and other high technology products
- Remarking and counterfeiting of computer hardware and software
- Intellectual property and trade secrets theft

Other organizations and jurisdictions may have slightly different definitions of high technology crime reflecting differences in priorities based on local crime patterns and other factors. The first comprehensive assessment in Britain identified nine types of computer crime:

Criminal communications	Electronic payments
Fraud	Gambling and pornography
Hacking	Harassment

[9] SB 1734, High Tech Crimes, 1998
[10] Parker, 1998, p. 72

Intellectual property offenses	Pedophilia
Viruses	

Hacking, viruses, child pornography and fraud were said to be well known problems while others such as cyber-stalking, blackmail by email, hate sites, work rage and gambling, are emerging types of crime.[11]

For the US Department of Justice there are three categories of computer crime:

- Computer hacking, including vandalism, disrupting the business of others, theft of intellectual property and trade secrets and government espionage
- Using a computer to commit a crime, such as child pornography and international counterfeiting (e.g. scanning and printing money)
- Traditional crimes, such as encrypting communications about criminal activity.[12]

Other U.S. Agencies focus on particular types of crime which may result in some overlap of jurisdiction:

- Customs Service - international child pornography, computerized cargo and EDI records; financial fraud, smuggling
- DEA - money laundering
- FBI - task forces on computer intrusion, network infrastructure protection, terrorism, wire transfer fraud, and child pornography in the US
- Federal Trade Commission - fraud
- IRS - money laundering, tax evasion
- Secret Service - telecommunications fraud
- Security and Exchange Commission - fraud, including securities fraud
- Treasury Dept. - counterfeiting, money laundering

[11] Hopkins, 1999.
[12] Burey, 1999

Characteristics of High Technology Crime in California

High technology crime in California varies by location and by various trends. Only in the last few years has it been determined that much of the chip and component theft and hijacking in Silicon Valley was orchestrated by ethnic gangs from Southern California. Sometimes the chips and components would be smuggled out of the country to be imported as products in the "gray market", which competes with legitimate locally manufactured products. This knowledge caused the high technology crime task forces to keep in close touch with other task forces monitoring gangs, hijackings and smuggling.

> *Combating high technology crime requires skills and resources that local police forces do not currently have.*

In recent years, Southern California has been known for its home invasions where a local manager is taken to his manufacturing plant or store to turn over computer products while his family is held hostage. This frightening crime, which is usually ethnically-oriented hasn't been seen in Silicon Valley for several years.

> *High technology crime differs between regions. Each region will have priorities and approaches that represent regional concerns and resources.*

As one type of crime is targeted by a regional task force, the perpetrators will shift their activities to another region, or another state.

> *High tech crime was viewed by many law enforcement agencies as a Silicon Valley issue until recently. The impact has been a delay in providing resources to address the matter. There is a real need to conduct more detailed studies to verify the scope and extent of high tech crimes.*

> *High technology criminals seem to be 2-3 years ahead of the technology capabilities of typical law enforcement agencies.*

According to the Search Group, in Sacramento, the latest trends in Internet-related crimes include:

- Various web site intrusion-related crimes
- Counterfeiting documents, including theft of identities
- On-line stalking
- Child exploitation

Child pornography is so big right now that it would consume our entire task force budget -- but we have to consider other crimes, too.

Regarding child pornography, FBI Director Freeh testified that:

- "The FBI has investigated more than 70 cases involving pedophiles traveling interstate to meet minors for the purposes of engaging in illicit sexual relationships."
- "Since 1995, the Innocent Images investigation has generated 328 search warrants, 62 consent searches, 162 indictments, 161 arrests, and 184 convictions."
- "…Since March of 1997, the number of search warrants executed increased 62 percent, the number of indictments obtained increased 50 percent; the number of arrests increased 57 percent; and the number of convictions increased 45 percent."
- "The 1998 Justice Appropriations Act provides $2.4 million to the Office of Justice Programs for grants to establish state and local law enforcement cyber-squads. This subcommittee also instructed that these cyber-squads follow the investigative protocols developed by the Department of Justice in the Innocent Images investigation."[13]

Potential evidence in child pornography cases is often kept on servers in foreign countries, out of the reach of local investigators.

High Technology Crimes Linked to Gangs

Chip, component and computer theft is often linked to cross-jurisdictional gang activity. Gangs from the Los Angeles area strike trucking yards, warehouses and loading docks in the Silicon Valley area to steal high tech items ranging from chips to powerful servers.

High technology crime is often linked to other types of crime. For example, Internet fraud or component theft is often linked with drug trafficking and gang activity. That's why Regional Task Forces try to investigate each high technology crime no matter how small.

[13] Freeh, 1998

A gang from South America is believed to be responsible for the theft of hundreds of millions of dollars worth of computer components from 45 Silicon Valley companies during the period 1997-1998. In fighting cargo theft, Silicon Valley law enforcement officials formed the Rapid Enforcement Allied Computer Team (REACT), the high technology crime task force for Silicon Valley.

> *Gangs, drug cartels and other forms of organized crime will use high technology crime as a supporting activity (money laundering) and as a way to raise funds.*

Local investigators may find even gangs operating from operating from off-shore, like insurance fraud syndicates operating from Eastern Europe through local contacts.

There is often a link between high technology crimes and other types of crime. The smallest high technology crime may lead to information about organized gang activity.

> *Law enforcement needs the tools and training to catch much of high tech crime before it occurs. Advanced technology will be required. Cybercrooks are far ahead of law enforcement in technology and capability.*

High Technology Crime Task Forces

The task force approach has been found to be preferred by local police jurisdictions around the country.[14] California currently has three high technology crime task forces in Sacramento, Silicon Valley and in Los Angeles-Orange Counties, with several others in formation. These task forces are described in Section 6.0.

In California the task force approach to fighting high technology crime has evolved from one-time collaborative efforts to fight high technology crime. According to Ohlhausen[15], this approach has been successful due to:

- Interagency communications and information sharing which allow the task force to operate as a clearing house to assign crimes to the task force or other agencies based on expertise and resources.

> *High technology crime is almost always multi-jurisdictional in nature and combating it requires approaches that are different from typical crimes within a*

[14] Meyer and Short, 1998
[15] Ohlhausen, 1997

jurisdiction. In particular, high technology crime requires a high degree of information sharing and coordination between police forces.

The Task Forces provide an opportunity for the close cooperation between federal, state and local law enforcement, since the representatives from each work closely together and, often, occupy the same office. Without this level of coordination, some types of high technology crime would be difficult to pursue.

- Relationships fostered by the task force approach and by other organizations such as the High Tech Crime Investigation Association (HTCIA) often contribute to a quick response to high technology crime.

Organizations like HTCIA which is comprised of federal prosecutors and agents, local prosecutors and police, and private sector security managers exist around the state; respond to a need to share information and learn, and form the grass root basis for the formation of Regional High Technology Crime Task Forces.

- Resource sharing assists local law enforcement officials who rarely have the right kind of high tech equipment. They usually have a mixture of items, often forfeited by convicted criminals.

Equipment is a major issue! Law enforcement personnel do not have access to the latest computers and equipment required for on-line investigation.

- Expertise of the talented police officers, attracted to the task force, who share their knowledge within the task force and with the surrounding police departments.

- "Big Picture" focus on the crime network which typically extends beyond jurisdictional boundaries.

While Regional Task Forces are based on geography, one suggestion is to have some Task Forces based on crime-fighting expertise, such as computer intrusion, or forensics.

- Financial Benefits of sharing resources between local, state and federal police and to a lesser extent with associated corporate members.

The task forces help resolve the different interests of local, state and federal law enforcement agencies, especially when representatives from these agencies work side-by-side on a daily basis.

There may be an inconsistency between federal and state high technology crime laws for certain crimes. This compounds the difficulties of local prosecution due to the use of thresholds by federal prosecutors, inter-jurisdictional differences and the lack of resources to pursue cases.

Forensic Evidence

Since the use of computers is increasing in society, virtually all crimes may have a high technology aspect such as the use of computers for record keeping or the use of E-mail in communications. Therefore every crime investigation should consider the possible uses of high technology and the possibilities presented for the collection of evidence.

> *Privacy is a big issue but legislation is needed to address the use of computer "fingerprints", the use of personal data in on-line activity and other related issues.*

The types of evidence computer forensics can provide include:

- Direct evidence of the crime itself
- Identities of co-conspirators
- Financial documentation of criminal activity
- Identity and/or location of the victim

> *Advanced computer forensics can be handled by the Task Force, large police departments or federal agencies. Simple computer forensics should be handled by the local police department since computer-related evidence may be present in nearly every crime.*

Thresholds and Prosecution

Like many crimes, high technology crimes are prioritized by the associated financial losses. Thus large scale crimes are almost always prosecuted but crimes with a loss below a threshold, set by U.S. Attorneys in each region, are often not prosecuted by the Federal government. This sometimes leaves local officials in the difficult position of deciding whether or not to prosecute a particular crime in the face of limited resources. In particular, multi-jurisdictional crimes, such as inter-state high technology crime, that are below the threshold are often beyond the capabilities and resources of local law enforcement officials.

> *While large cases are handled by the FBI, and other federal agencies, mid-size and small cases are not adequately addressed due to the application of thresholds to prioritize crimes.*

Since Internet-related crimes can be perpetrated from virtually anywhere, the use of thresholds poses a potentially difficult problem for local law enforcement.

High technology crime tasks forces have begun to address this problem through the realization that many high technology crimes, often too small for prosecution, may be linked to other crimes. Therefore each crime is carefully reviewed and even if it doesn't lead to an arrest, it may lead to another crime that can be prosecuted.

Crimes involving the public "at large" may also present a prosecution problem. Unless the losses due to some types of high technology crimes such as telecommunications and cable signal theft can be aggregated, or linked to organized crime, then it appears that they will not be pursued as vigorously as other types of high technology crime.

> *The best approach to fight high tech crime is the use of deterrents. Traditional law enforcement does not take action until the crime has already been committed, then the criminal is sought, Deterrents would take the form of fear (of getting caught), disapproval (thought of as a criminal), and value (low net value of what is stolen). Creating a belief that high tech crime doesn't pay is the better approach.*

The Value of Information

Since high technology crimes are prioritized for prosecution based on the value of the loss suffered, some relatively important crimes may not be prosecuted since no dollar loss occurs. For example, the theft of social security, credit card and bank account numbers won't be prosecuted until someone uses the information to commit fraud. Organizations with databases holding large amounts of important information may not be able to get assistance to stop electronic theft or to prosecute the thieves since no monetary loss has occurred. Under the current implementation of the law, there is no difference between types of information that are stolen.

Computer and Network Risk

Computer and network risk is based on the cost of site security versus the potential loss associated with loss of service, site damage or monetary loss. In 1997, Dan Farmer, co-developer of the Security Administrator's Tool for Analyzing Networks (SATAN), lightly probed 1,734 web sites and found that over 60% could be broken into or destroyed. Only three sites questioned his activity. Presumably the vast majority of sites did not even detect it.[16] And

[16] Farmer, 1996

the situation may not be much better today. A recent survey of 359 Information Technology managers by Zona Research found that less than half of the managers protected their sites with hardware firewalls or intrusion detection (considered essential by most experts), while 4% had no security protection at all![17] Friendly penetrations of corporate and government web sites continue to demonstrate their vulnerability to outside attack.

While this risk may be easily understood for individual web sites, it is less so for the public network. In 1998, seven hackers testified before Congress that it would only take 30 minutes for them to render the Internet unusable for the entire nation.[18] The protection of the Internet, numerous networks around the world interconnected with a common protocol, may not be possible. The FBI's National Infrastructure Protection Program, among others, has as its mission to protect this and other vital utility systems.

Gray Market Risk

The theft of chips, components and computers, and the piracy of software has an added risk of great importance to California. These items are usually sold back into the market in competition with the California firms that originally produced them.

> *Stolen computer chips can change hands, from state to state and internationally, very rapidly. They can move from theft to assembly into a black market PC rapidly. It is nearly impossible today to follow such rapid movement since chips are not marked with ID numbers.*

In this market, known as the gray market, the criminal often modifies components such that they wear out faster than expected, or remarks them so that the buyer believes that he or she is getting a better product. This underperformance by gray market goods also may impact the brand under which they are sometimes illegally sold.

> *The "Gray Market" fuels the demand for the theft of chips and components, which are sold in competition with legitimate products.*

The potential economic impact of lost revenues and jobs, and foregone sales taxes and income taxes, associated with the gray market could be very large. Therefore recent California legislation, such as SB 1734, has emphasized the gray market as a high technology crime issue.

[17] Information Week, May 31, 1999, p 112
[18] Yasin, 1998

Crimes linked with gray market activity include home invasion robberies, hijackings and other crimes associated with gangs and organized crime.

Where is the Gray Market"?

Stolen goods are remarked, built, modified or rebuilt into computer products, often under well known labels. Sometimes the goods are sold to manufacturing companies as legitimate goods. These stolen goods end up being sold back to companies and the public through:

- Computer stores (selling into legitimate distribution channels)
- Bulletin boards / classified ads
- Computer shows / mail order catalogs
- Flea markets / second hand stores / street dealers

Unusually low, yet unadvertised, prices are usually a tip-off to gray market goods.

The Evolution of Hackers

The Internet is a training ground for young computer experts interested in breaking into the computer systems of others. With this training, the "hacker" may decide to sell his or her services for various illegal activities.

Script Kiddies and the Experts

Novice hackers begin their exploits by downloading small programs, or scripts, designed to penetrate various types of hardware and software environments. Armed with these scripts, and often little other knowledge, these "script kiddies" begin to hack into systems worldwide. These scripts are written by a relatively small number of experts, believed to number less than a hundred persons.

> *It is estimated that there are less than 100 programmers in the world with enough expertise in software, systems architecture and hardware to write programs to intrude into Internet and related systems. Many thousands of others download their programs from the Internet for use in the commission of Internet-related crime.*

When a hacker breaks into a site to place slogans or the disable features, they appear to believe that the fix will be as easy as the break-in. But in fact a brief break-in can cause a long period of recovery.

> *While the hacker may have rewritten an 8K HTML file in ten minutes, the owner of the site must review each line of code on the web server, keeping an eye out for*

> *trap doors, Trojan horses and other hacker tactics -- a process that could take weeks and be very expensive.*

Damages can be extensive. For example, several high tech companies claim that Kevin Mitnik cost them $291 Million in damages, although others dispute these claims.[19] In any case, there is mounting evidence that these break-ins are costly to companies.

A 1998 study of Fortune 1000 companies by WarRoom Research found:

- the vast majority of companies had experienced a break-in by an outsider in the past year
- more than half the companies had experienced more than 30 system penetrations in the same time period
- nearly 60% said that they had lost $200,000 or more as the result of each intrusion.[20]

The results of the 1999 CSI/FBI Computer Crime and Security Survey, in general, confirm these findings. Thirty percent of the 163 respondents reported intrusions by outsiders and 55% reported unauthorized access by insiders that resulted in over $120 million in losses.[21]

The Profit Motive and Economic Espionage

The promoters of the world's largest hacker conference points out a trend that where hackers use to appear to hold a code of ethics, now they are beginning to hire themselves out to perform corporate espionage.

The rapid development and acceptance of the Internet has given new opportunities for corporate or economic espionage. Typically the theft of intellectual property or trade secrets is caused by:

- Disgruntled employees, who sell secrets and disrupt plans
- Other domestic and multinational corporations for competitive information
- Foreign governments in countries where corporations are owned by or closely tied to the government for the purposes of gaining economic advantage and enhancing economic development

[19] Miller, 1999
[20] Wilson, 1998
[21] Computer Security Institute, 1999

- Foreign governments to gain defense secrets from defense contractors

These companies and governments may increasingly seek out the services of a knowledgeable hacker.

This attack on intellectual property gave rise to the Economic Espionage Act of 1996 which makes the theft of trade secrets a federal criminal offense.

Discovering, Measuring and Reporting High Technology Crime

Every interview conducted for this report and virtually every source of information uncovered on the subject implies that its level is high and is growing rapidly. However, for various reasons there are insufficient data about high technology crime. Most of what is known is anecdotal; the rest is based on surveys which have readily admitted biases.

Many experts have said that 9 out of 10 computer break-ins are unreported[22], this number appears to be rising according to the 1999 CSI / FBI survey.

> *The amount of high technology crime, especially where it is related to access to the Internet, is not precisely known and may not be knowable in a democracy.*

The reasons often presented for the under reporting of high technology crime are:

- Private companies prefer to handle cases internally to avoid embarrassment and adverse publicity.

> *Police Departments have little information as private companies are unwilling to share information on high tech crimes. Most use private security firms or have in-house security organizations. Private firms do not want information released to the public.*

> *Legislation is needed to restrict certain high tech criminal data from becoming public information. Unless we do this we will never have a clear picture of this rapidly growing area of crime.*

- Insiders are often easier to catch than outsiders. Additionally, the company may want to make an example out of an insider, whereas to pursue conviction for an outsider

[22] Kabay, 1998

may give the appearance that the company can't follow its own security policy and can't control its security.

High technology crime is often not reported by the victimized corporations for various reasons such as fear of bad publicity, perception of a low likelihood of success based on previous prosecutions, the amount of company work involved in the prosecution of a case, and finally, its analysis as a business decision - it may be less expensive to take the insurance coverage on the loss.

- Companies may decide not to prosecute or report a crime due to cost considerations.

It can be expensive for a company to prepare evidence for use in a prosecution.

- Most computer abuse is probably not discovered[23].

High technology crime is difficult to detect. Sometimes even the victim doesn't know a crime has been committed.

- Surveys of high technology crime are often unscientific and ambiguous making it difficult to interpret the data.

We need well-trained criminal intelligence analysts to pull together the bits and pieces of information we collect. Information collection is not much good without an analysis process.

Another problem with the reporting of high technology crime is the absence of an established reporting system which indicates that a crime is in fact high tech.

High technology crimes are often classified as a theft or a fraud which leads to a lack of valid statistics of reported crime.

"Comprehensive crime statistics involving electronic money and computer fraud and abuse are difficult to obtain. The FBI is working closely with federal banking regulators and the financial institution industry to evaluate methods by which computer related activity can be statistically tracked and monitored in order to assure that fraudulent activity of this nature is reported. The Suspicious Activity Reporting System (SARS), currently used by financial institutions to report fraudulent activity could be used, with some minor modification, to provide a simple and straightforward means for victims to report this increasing crime problem. The FBI and federal

[23] Kabay, 1998

bank regulators have already worked together to provide guidance to the financial industry for reporting of computer crimes on SARs."[24]

The lack of an established reporting system could also be resolved if the Uniform Crime Report form could be changed to reflect a high technology crime. Although presumably costly to implement, it may prove to be a cost-effective way to track high technology crime.

> *The Uniform Crime Report should have at least a high technology crime "block" to check in order to begin to generate information on these crimes. According to one source this would take "millions" of dollars and so the suggestion has not been seriously considered.*

The Importance of Reporting High Technology Crime

There is a reticence among the private sector to share information about high technology crime. Among manufacturers, this reluctance may be overcome by the realization that it happens to everyone and doesn't usually affect the public image of the company. For service companies, however, the problem is real. The perception that an organization such as an on-line bank or an electronic commerce site is susceptible to high technology crime may lead to a real impact on its bottom line. In this case there is a need for secrecy when a company cooperates with an investigating law enforcement agency.

> *Legislation is needed to restrict certain high tech criminal data from becoming public information. This is the only way we will ever have a clear picture of this rapidly growing area of crime.*

Because high technology crime is under-reported, local law enforcement is not allocated the resources they require to fight it. And since high technology crime is more complex and costly to investigate than conventional crime, it has been suggested that corporate security managers be certified or licensed, or that standards for reporting high technology crime be jointly developed by the public and private sectors[25]. This could tie into the government's policy on "information warfare" where the private sector bears the burden of its own security while the government protects the public network.

> *There is a strong need to address mandatory reporting of high tech crimes to provide a basis for legislation and funding. Perhaps the reluctance of private sector reporting can be overcome if the information is not available to the public or if it is not specifically identified to the reporting firm.*

[24] Gallagher, 1998
[25] Mitchell and Banker, 1998

Approaches to Measuring High Technology Crime

Most officials feel that information about past high technology crimes is largely not available and that we should now begin to collect information. One person suggested a one-time detailed survey, followed by annual reporting to update it.

Actually the three existing task forces have begun to collect data as noted in a following section. The enabling legislation, SB 1734, also requires that data be collected and reported by the task forces on an annual basis. This data will include:

- the number of high technology crime cases filed in the prior year
- the number of high technology crime cases investigated in the prior year
- the number of victims involved in the cases filed
- the number of convictions obtained in the prior year
- The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained
- the amount of funds received and expended in the past year
- the uses to which those funds were put, including the payment of salaries and expenses, purchases of supplies, and other expenditures of funds

However, the key data for investigators will become available over time as the High Technology Crime Database is established. As described in Section 8.0, this database will allow investigators to track incidents throughout the state.

But on the question of encouraging corporations to report high technology crime, it may be necessary to set up a national reporting and tracking system, such as the system developed by the Center for Disease Control, that would collect and assess information on disparate security incidents.[26] Perhaps more acceptable would be an anonymous reporting system such as the Flight Incident Reporting System maintained by NASA to track flight incidents without attribution or publication -- and where anyone can make a report.

[26] described by the Rand Corporation in *The Day After in Cyberspace*

Training to Fight High Technology Crime

There is a fundamental problem of providing qualified high technology security personnel to the private sector. Based on a survey of 552 security managers, the American Society of Industrial Security (ASIS) predicts an increasing demand for high technology security professionals.[27] But these professionals simply may not be available. It is currently estimated that there is a nationwide shortage of about 360,000 information technology workers and that the annual demand is about 95,000 workers, of which approximately 50,000 could come from computer science and related IT university and college programs, and the remaining 45,000 from retraining workers.

> *We must train for the whole security system, not just the technical components. There's currently a focus on the technology of encryption, but if an unauthorized person gets hold of the encryption keys -- it's over.*

Or perhaps corporations can lure qualified law enforcement officials from their public jobs to fill in some of their requirements. However, for law enforcement there is a very important need to continually train and upgrade the skills of qualified peace officers, such as those found on the high technology crime task forces as well as the average policeman.

> *Training is a major issue! Law enforcement personnel lack the technical training to deal with high tech crimes.*

> *Basic computer forensics can be part on any crime investigation and must be part of each police force's capabilities. On-the-job training in basic forensics and other introductory high technology crime subjects can be provided to local forces by the Regional High Technology Crime Task Force.*

Finally, public education may be the best approach to fighting crimes such as the theft of cable television services which is committed by large numbers of people.

> *There is a need to educate the public about high technology crime.*

[27] Radcliffe, 1998

The Future of High Technology Crime

Some aspects of high technology crime are sure to grow as computers and access to the Internet become more wide-spread. In addition, as the use of the Internet will continue to evolve and grow in many areas such as:

- Electronic commerce
- On-line banking
- Drug stores with prescriptions services
- Health care services and records
- Education

High technology crime will continue to change over time as technology and its uses change.

As computers become smaller, even wearable, and as communications access becomes more available new applications will certainly lead to new types of crime. Also, as computers and components become smaller, their value per unit volume may continue to grow and result in continued product thefts.

4.0 TYPES AND COSTS OF HIGH TECHNOLOGY CRIME

In the following sections each category of high technology crime is examined and the associated published costs of crime are presented.

White-Collar Crime

High technology white collar crime, or economic crime, cons
committed by means of electronic or computer-related media.
computers in business, much of white collar crime is high tec
types of fraud such as:

- Bank fraud, including automated teller machine fraud
- Credit card fraud (often with stolen credit card numbe
  commerce
- Insurance fraud
- Stock market and other investment-related fraud

"A recent Internet survey indicated that electronic banking is
next two years... In the latter part of 1997, the Federal Depos
that over 1,100 banks and thrifts were maintaining a presence
August, 1996 Financial Times report cited a "survey of Intern
European Banks had web sites and that the rate of banks com
90% a year.[30]

Increasing levels of on-line fraud can be expected in the rapid
commerce. A recent Information Week and Pricewaterhouse
challenge ahead: "Overall 59% of sites selling products or se
or more security breaches in 1998. 84% say they lost betwee
dollars. The other 16 percent say they each racked up more th

Another indication of the difficulty of doing business on-line
International is that while only 2% of its business is done on t
its disputes.[32]

The suspect (age 17) was able to download 850 credit card numbers from a major internet service provider (ISP). One of his methods was to send email to ISP customers who thought they were from the ISP accounting department. He then posted the numbers on the Internet to share with others. He and his colleagues then used the credit accounts to make on-line purchases of goods and services. (1999 activity report of the Sacramento Valley High Tech Crimes Task Force.)

A former tax preparer threatened to sell the financial information, including identity and credit documents, of 22 former clients on the Internet unless they paid him $150 each. (Sacramento Bee, July 12, 1997)

"With my criminal mind and a computer, I don't need a job," the 32-year-old suspect allegedly boasted to a friend. Certainly by the time he was arrested by San Mateo County Sheriff's deputies, he had been thought to have used his hi-tech skills to steal more than $50,000 - and possibly as much as $1million - from the bank accounts of a dozen or more victims. (Network Week Online, November 26, 1997).

[28] See Section 13848 (b)(1) of the California Penal Code
[29] Vatis, 1999
[30] Gallagher, 1997
[31] Business Wire, March 22, 1999
[32] Computerworld, March 26,1999

A 1999 study for the National Consumer League found that 7 percent of web users, or 6 million users, reported online fraud or misuse of their credit card.[33] An earlier National Consumers League report states that more than 100 scam complaints, ranging from $10 to $10,000 in size, are received each month involving Internet fraud. Complaints involve undelivered services, undelivered merchandise, pyramid schemes, multi-level marketing, misrepresented business opportunities, work-at-home schemes, credit card schemes, books and magazine subscriptions.[34]

> *Internet fraud is considered the major problem that should have priority. On-line rip-off crimes focused on children are the big issue today.*

White-Collar Crime Published Costs

In the 1999 CSI / FBI survey the average company responding to the survey had $1.47 million in losses from on-line fraud. Certainly, the average amount per consumer is much lower, but is still significant due to the numbers of on-line consumers.[35]

The 1999 CSI / FBI survey also noted that the average level of fraud is increasing over the previous two surveys.

[33] Louis Harris and Associates, 1999
[34] Gallagher, 1997; Ohlhausen, and Parker. For E-commerce fraud see Dalton, Owens, and CSI
[35] If 1% of the $50 billion in e-commerce transactions were fraudulent and if these losses were suffered by 6 million persons, then the average amount in dispute per transaction would be approximately $83.

Computers and Networks

Computer and network crime is based on computer and netv
unlawful access, destruction or unauthorized entry into and
government computers and networks, including wireless and
and law enforcement dispatch systems, and the theft, interce
unauthorized disclosure of data stored within those compute
category commit a range of crimes, such as:

- Child pornography / child exploitation / on-line sedu
- Cyber-stalking
- Cyber-terrorism
- Denial of service / spam
- Espionage / theft of valuable information such as pas
  competitive information
- Hate sites / hate crimes
- Identity theft / counterfeiting (documents)
- Tampering with information such as employee, educ
- Vandalism - hacker activity / web site damage and d
- Virus dissemination

Most intrusion is the result of insiders, but the trend is towar
According to a Meta Group study of more than 520 informa
60% of the current security violations were internal but this
the year 2000.[37]

The suspect hacked into a UC Davis computer system and stole several email accounts. He then used these accounts to order computer components using stolen credit card accounts which he obtained by stealing mail. Two days of surveillance paid off when he was arrested while attempting to pick up deliveries.

The task force was called out to assist with a vehicle stop where the detainee, on probation, was wanted in connection with the identity takeover of a probation officer. A laptop computer and computer-generated counterfeit checks and identification were recovered from the car.

Assisted in an investigation where the suspect registered an Internet domain name of "Folsom High Must Die" and made the web site appear to be the work of a local police detective.

Assisted an Oregon police department to investigate three juvenile suspects who had conspired to shoot and bomb students and faculty during a graduation ceremony. Seized computers obtained evidence of the conspiracy.

(1999 activity reports of the Sacramento Valley High Tech Crimes Task Force.)

[36] See Section 13848 (b)(2) of the California Penal Code
[37] Information Week, March 16, 1999

Local police appear to be better able than federal officials to distinguish and handle suspects performing pranks or vandalism from more serious criminals, although the vandals do not usually understand how their actions can result in significant costs to the hacked site.

In Congressional testimony, Mr. Vatis cites published statistics relative to computer intrusion:[38]

- "A study of 300 Australian companies by Deloitte Touche Tohmatsu found that over 37 percent of the companies experienced some form of security compromise in 1997, with the highest percentage of intrusions (57%) occurring in the banking and finance industry."

- "A 1996 survey of the American Bar Association of 1,000 companies showed that 48 percent had experienced computer fraud in the last five years. Company losses were reported to have ranged from $2 – 10 million."

- "In 1996, the Defense Information Systems Agency (DISA) estimated that as many as 250,000 attacks on DOD systems may have occurred in 1995. DISA indicates that the number of attacks has been increasing each year for the past few years, and that trend is expected to continue."

In one form of high technology crime, person impersonation or stolen identity (e.g. social security and credit card numbers), the victim must prove his or her innocence, a process that might take years, exhaust the victim's savings and ruin his or her credit. The victim must hire an attorney and convince federal, state and local agencies, and financial institutions that they did not incur the alleged debts or owe taxes on wages or transactions benefiting the perpetrator. It is recommended that a law be passed to protect the victim of this type of crime.

Identity theft is often accomplished by experienced thieves using the following methods: "Prextexting", or posing as the consumer to obtain proprietary bank account information and "skimming" the magnetic strip on the ATM or credit card to read and store customer information that is later transferred to another card, identical to that of the victim. The Congressionally approved "Identity Theft and Assumption Deterrence Act of 1998" strengthens laws governing theft of identity."[39]

[38] Vatis, 1999, p. 5
[39] Bernstein, 1999

Privacy is a big issue. Legislation is needed to address the use of computer fingerprints, use of personal data in on-line activity and other related issues.

Files of illegal pornographic images are placed on the servers of unsuspecting organizations and copies are kept on a safe off-shore server. Records of toxic chemicals are altered in databases so that they may be dumped without concern of prosecution. And prescription drugs are illegally sold on the Internet, often in violation of other (e.g. import - export) regulations.

What kind of damage can a hacker do?[40]

- Denial of service attacks in which a site is flooded with hundreds of incomplete Internet connections per second, causing the server to analyze and respond with an error message, thus fully occupying the server's processing time in an attempt to deny other users access or to cause the server to crash

- Accessing and stealing user passwords, credit card numbers and other sensitive information

- Causing a destructive virus (e.g. erases local hard disk) to proliferate via web site links and/or email

- Tampering with a web site; defacing graphics and placing links to undesirable sites

- Placing trap doors on a web site which allow easy return access

Computers and Networks Crime Published Costs

The average costs per firm responding to the CSI / FBI survey are over $100,000 per attack.[41] Although estimates of $3 billion per year in damages from computer and network crime may seem high, [42] a recent study based on185 companies with 900,000 network users estimates that virus attacks cause in $7.6 billion in losses to business.[43]

According to the Meta study, 520 information technology firms are spending an average of $2.8 million each on computer security, a total of nearly $1.5 billion.[44]

[40] Angelica, 1998
[41] Denial of service: $116,000, Virus attack: $45,000, Insider abuse: $143,000, Outsider Intrusion: $103,000, Sabotage: $164,000
[42] Angelica, 1998
[43] Reuters, 1999
[44] Information Week, March 16, 1999

Money Laundering

Money laundering includes the illegal transfer of funds a
networks or electronic banking transfers.[45] Included in th
counterfeiting of negotiable instruments and other valuab
technology.

From April 1998 to the present, the suspects have engaged in a double invoicing scheme that has defrauded the United Kingdom out of about $30 million in taxes. UK and US Customs agents are investigating with assistance from REACT. (From a REACT case summary sheet, March 23, 1999. REACT is the High Tech Crime Task Force operating in the Silicon Valley region)

Electronic cash[46], smart cards and the off-shore location
increase the potential for high tech money laundering. L
downloaded from an ATM to a smart card and then be tr
any records. Money launderers will not need to enter mo
not need to carry around bulky amounts of cash.[47]

> *The use of the Internet in the commission of crime is becoming more sophisticated. Money, often fraudulently obtained, is moved in and out of the accounts of unsuspecting businesses and financial institutions until it is "laundered" or reaches an untouchable off-shore location.*

Aside from the international wire transfer of funds[48], the use of high technology in money laundering is considered to be growing rapidly but is not yet the predominant .

Money Laundering Crime Published Costs

An estimated $500 billion is laundered globally each year, although exact figures are not given out by the investigating agencies.

[45] See Section 13848 (b)(3) of the California Penal Code
[46] Also E-cash or digital cash. Smart cards and digital coins are forms of digital cash.
[47] Fisse and Leonard, 1997
[48] estimated to be on the order of trillions of dollars each day

Telecommunications and Cable Television Services Crime

Crimes in this category include the theft and resale of te
telecommunications service, theft of wireless communi
television services by manipulation of the equipment us

Los Angeles County Sheriff Department investigators seized several hundred descrambler boxes and related equipment. A suspect was caught manufacturing and selling modified cable descrambler boxes after installing special EPROM (electronic programmable read-only memory) and "Quickboard" devices inside standard cable TV reception boxes. (Taken from a Department report, February 1999)

Telecommunications and Cable TV includes wireline a le
and satellite TV services

*Some high technology crimes are seemingly con
scramblers" which are made for the illegal theft
over 50 magazines and are available for purchase from an increasing number of web sites.*

Where public demand is involved, it is easier to reduce demand through a public education program ("send a strong message") about high technology crime and its consequences, than to kill supply.

A study by the Anti-Theft Cable Task Force found the following:

- "Piracy costs operators more than $6 billion annually, not even including unrealized pay-per-view revenue, according to the National Cable Television Association."
- "More than 11 percent of the 94 million cable homes passed are stealing signals, and about 9.23 percent of homes are stealing premium services, according to the report, which was obtained by Multichannel News."
- "…An average 100,000-subscriber system loses about $7.16 million per year due to theft…just converting theft of pay services could realize a system $500,000 per year, according to NCTA and task-force estimates."
- "It's hard to quantify theft because people don't let us into the house," Gordon said. "But if you take the conservative numbers that we have, this is a problem that's costing operators in excess of $10 billion."[50]

[49] See Section 13848 (b)(4) of the California Penal Code
[50] Umstead, 1998

Telecommunications Services Crime Published Costs

Telecommunications and cable fraud consists of wireline, wireless and cable / satellite fraud:

- Wireline: In 1997, long distance service fraud in the US climbed to over $4 billion with approximately 30% in California.[51] Landline calling card fraud is $1billion in US, approximately 30% in California: $300 million.[52]

- Wireless: $1 billion in US in1996, but now down to $300 million. The California market losses went from $150 million to $40 million during the same period.[53] It appears that wireless fraud is declining. "In 1997, the wireless industry lost $644 million due to fraud, or 1.4 percent of total industry revenues. It is estimated that losses for 1998 will be 182 million or 0.05% of industry revenues."[54]

- Cable: A survey prepared for the California Cable Television Association reveals that in 1998, California cable operators lost over $741 million to theft of basic and premium services.[55]

- 1999 CSI/FBI Survey: The average telecom theft loss per firm is $27,000.

[51] Telecom and Network Security Review, April 1997
[52] Source: California telephone company
[53] Source: California wireless communications company
[54] Bell Atlantic, 1997
[55] C&R Research, June 1999

Software Piracy

Software piracy includes the illegal copying of software, of information.[56] Included in this type of crime are the:

- creation and distribution of counterfeit software
- use of counterfeit trademarks to misrepresent the
- motion picture industry piracy
- music industry piracy
- and the creation and distribution of other counterf

Piracy is the major problem of software developers. Acc and the Software Publishers Association study, of the 61 applications installed worldwide during 1998, 231 millio represents an increase of 2.5 million more applications th

"Revenue losses to the global software industry due to pi North America, Asia and Western Europe accounted for Microsoft claims to have lost $7.6 billion and Adobe, $4

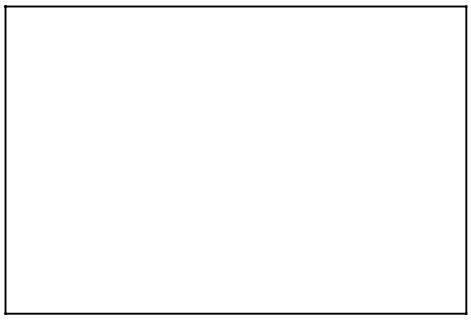
"Software piracy committed in the United States is a sev ss applications alone in the United States resulted in softwa o $3 billion in retail sales. Since 1994, business software p publishers about $12 billion."

The Business Software Alliance (BSA) announced that five California organizations in the Los Angeles area have agreed to settle claims relating to unlicensed copies of software programs installed on office computers. Combined, the companies will pay over $600.000 to BSA. California is already the State leading BSA recoveries, with over $6 million paid by organizations since 1993. (BSA Press Release, February 24, 1999)

"Major Hollywood studios including Universal City Studios, Paramount Pictures, Metro-Goldwyn-Mayer Pictures, United Artists, Columbia Pictures Industries, Warner Bros., Disney Enterprises and 20th Century Fox Film Corp. filed a copyright-infringement lawsuit against four individuals for allegedly selling hundreds of pirated videocassettes through a national telemarketing scam. This follows a three-year investigation by the Motion Picture Association of America (MPAA) who also received tips from dealers who were suspicious of the telemarketed offer and called the organization's piracy hot line. The telemarketers operated under several names, including R&R Products Corp Carousel, CA Productions, AKC-Best scam ran in 39 states, covering hundreds stores and 329 video titles.
Of the 200 stores that had purchased the allegedly illegal product, dealers with no prior history of selling pirated material were given

[56] See Section 13848 (b)(5) of the California Penal Code
[57] BSA, 1999

"Piracy is committed in many ways: between friends and co-workers who want to share the latest products or by businesses seeking to reduce costs or through illegal rental, counterfeiting, and increasingly over the Internet. Regardless of how or where it occurs, piracy affects more than just the largest software publishers. Of SIIA's (Software Information Industry Association) over 1,200 member companies, 60 percent have annual revenues of less than $2 million."[58]



"Software piracy, as well as all other types of piracy, continues to be an international concern. According to the International Intellectual Property Alliance, copyright piracy cost an estimated loss of $10.8 billion to U.S. copyright industries. In addition, the International Anti-Counterfeiting Coalition has estimated that the cost due to trademark infringement in the world to be $250-350 billion. U.S. industries represent the leading edge of the world's high technology, entertainment, and apparel industries. Piracy of copyrighted and trademarked items cost the U.S. economy tax revenue and jobs because of the manufacture, distribution and sale of counterfeit goods."[59]

"Colleen Pouliot, senior vice president and general counsel for Adobe systems, told a hearing of the trade subcommittee of the Senate Foreign Relations Committee: "The software industry currently employs well over a million people and generates more than $28 billion in tax revenues. However, if software theft was eliminated in the U.S. and substantially reduced abroad, the software industry could produce an additional one million jobs by 2005 and raise an additional $25 billion in government revenues."[60]

"Sandra Boulton, director, piracy prevention at Autodesk estimates that piracy cost California alone some 18,900 jobs and $2.5 billion in lost wages, retail sales and tax revenues last year."[61]

"The copyright industry has lost millions of dollars due to piracy of software, music, and interactive digital software on the Internet. Hundreds of digital jukeboxes are surfacing on the Internet. The digital jukeboxes release music over the Internet in the form of MPEG3 digitally compressed files, called MP3s, which can be downloaded free of charge on to home computers. Most pirate jukeboxes are run for free by young music buffs, often students using university servers. Downloading music free of charge from the Internet is becoming increasingly popular

[58] Starback, 1999
[59] Gallagher, 1998
[60] Holland, April 17, 1999; Clausing, April 30, 1999
[61] Hines, 1998

among 15 to 30 year olds who tend to be frequent record buyers and are often computer enthusiasts. The record industry now stands to lose substantial sums of money because of the unauthorized distribution of its copyrights."[62]

"Major Hollywood studios including Universal City Studios, Paramount Pictures, Metro-Goldwyn-Mayer Pictures, United Artists, Columbia Pictures Industries, Warner Bros., Disney Enterprises and 20th Century Fox Film Corp. filed a copyright-infringement lawsuit against four individuals for allegedly selling hundreds of pirated videocassettes through a national telemarketing scam. This follows a three-year investigation by the Motion Picture Association of America (MPAA) who had also received tips from dealers who were suspicious of the telemarketed offer and called the organization's piracy hot line. The telemarketers operated under several names, including R&R Products Corp Carousel, CA Productions, AKC-Best Products, Bit Productions, OSG Enterprises, OSG Videos and IHC. The MPAA alleges the scam ran in 39 states, covering hundreds stores and 329 video titles. Of the 200 stores that had purchased the allegedly illegal product, dealers with no prior history of selling pirated material were given the option return the pirated copies on a voluntary basis. Other stores that had a history of selling pirated copies were sued by the MPAA in civil court. The MPAA member companies are seeking unspecified financial damages from the principles named in these allegedly illegal businesses, and permanent injunctions against further duplication and distribution of the copyrighted material."[63]

"While cassette piracy in the U.S. is down for the fifth year, CD, CD-R and Internet piracy is on the rise according to the RIAA's 1998 year-end anti-piracy statistics report released in April. The statistics on counterfeit, pirate, and bootleg CD-R seizures skyrocketed from 442 in 1997 to 103,971 in 1998, the piracy fueled by an influx of inexpensive CD-R hardware and blank discs. The RIAA ... sent out thousands of warnings and cease-and-desist orders to owners of music sites and initiated or already settled five lawsuits against online music-site pirates. Arrests and indictments were up from 211 in 1997 to 324 last year. Guilty pleas convictions were also up, from 150 to 204 as were piracy-related judgments and settlements, from 6 to 10."[64]

Software Piracy Crime Published Costs

Software: A recent report on software piracy and counterfeiting in California estimates that losses to the State amounted to $2.5 billion in lost wages, tax revenues and retail sales. In addition the report claims that 18,900 jobs were lost.[65]

[62] Gallagher, 1997
[63] Fitzpatrick, 1999
[64] Bailey, 1999
[65] Microsoft, 1999

Motion picture piracy: The MPAA indicates that $250 million per year in the US and between $2-3 billion per year worldwide are lost to motion picture piracy.[66]

Theft and Resale of Computer Components and Other High Technology Products

Theft and resale of computer components and other high technology products produced by the high technology industry.[67] Included in this type of crime are the robbery or theft and resale of:

- Chips / microprocessors
- Components, including "boards"
- Computers

A major impact of this type of crime is the support of the "gray market" with its adverse economic impact on the California computer industry.

Rand undertook a thorough study of this type of crime, analyzing the losses of 95 firms from October 1997 to June 1998. Much of this crime is conducted by organized groups. Also, as pointed out in the Rand study most of the robberies occur while the goods are in transit Associated crimes include home invasion robberies and other crimes associated with organized groups.

Fraud in the sale of used computers has hit California manufacturers, according to the March 19, 1999 Sacrament Business Journal. Extensive probes of 10 refurbished computer sellers - eight in California, one in Dallas and one in Bellevue, Washington - revealed that manufacturers have lost an estimated half billion dollars over the last six years according to the Sacramento Valley Hi-Tech Crimes Task Force

One law office employee in San Francisco stole 2,000 laptop computers worth $1 million, then sold them through newspaper ads.

Another San Francisco company has lost $1 million in laptops since 1991. (AP, March 10, 1999)

70% of the theft of chips and components in Silicon Valley may be attributed to employees, ex-employees or contacts of employees.

Published Costs: The Rand study estimates the direct annual costs to be $247 million, nationwide.[68] Including indirect costs, the total national loss to manufacturers is $1 billion. The total direct loss from non-manufacturers (largely customers) is estimated to be at least $4 billion, for a total cost of $5 billion, or $4.25 billion in direct equipment losses. It also estimates the "per incident" cost at $20,000. The 1999 CSI / FBI survey reports the average firm's laptop theft cost to be $87,000.

[66] MPAA, 1999
[67] Section 13848 (b)(6) of the California Penal Code
[68] Rand, 1999

Remarking and Counterfeiting of Computer Hardware and Software

Remarking and counterfeiting of computer hardware and software.[69] This type of crime is usually related to the theft and resale of chips, components and computers and contributes to the existence of the gray market.

This crime involves the repackaging and possible rem
usually only undertaken by organized groups working
accounts for large losses and has a serious impact on t

Feds Break-Up Counterfeit Ring
(SANTA ANA) -- A federal task force in Orange County has broken up a massive computer software counterfeiting ring. Twelve suspected software pirates have been indicted by a grand jury on charges of operating the large-scale multi-national counterfeiting and money laundering scheme out of Westminster. A federal prosecutor says the defendants illegally manufactured Microsoft computer programs, such as Windows '98 and Office '97. In one day, 56 million dollars worth of the phonies were manufactured. (Yahoo News, Friday June 4 , 1999.)

Published Costs

The costs for remarking hardware are included in the
counterfeiting software are included in the section on

[69] Section 13848 (b)(1) of the California Penal Code

Trade Secrets

This crime includes the theft of trade secrets[70] and other
secret theft can be a traditional theft of critical informat
electronic theft, related to network intrusion

The theft of intellectual property and trade secrets has b
network and computer intrusion.[71]

As previously mentioned, there appears to be a trend an
break into web sites and steal intellectual property and t
including international corporations, and foreign goverr

In one of the nation's largest computer frauds the company has been victimized by bribery, deceit and theft of a closely guarded trade secret, according to federal prosecutors. The rip-off has cost the company "tens of millions" of dollars according to a company investigator and a former Roseville police expert in high-tech crimes.

Put simply, the case involves stealing top-secret software, copying it, selling it, then using it to upgrade computer servers - which are powerful computers that feed information to a network of other computers, typically workstations. (taken from the Sacramento Bee, April 24, 1999).

*Some high technology crimes do not have a direct m
very serious, such as the stealing of trade secrets ar
of sensitive information. Although against the law,
priority investigations.*

Companies have a very difficult time attempting to estimate the value of a trade secret.

Companies struggle to place a value on certain types of crime such as the theft of trade secrets, while law enforcement response will often depend solely on the dollar amount of the loss.

Technology manufacturers are reluctant to reveal proprietary information and trade secrets to law enforcement based on the concern that it will get into the hands of competitors. This information could be helpful to law enforcement.

[70] Section 13848 (b)(1) of the California Penal Code
[71] Swartwood, 1997
[72] Wilson, 1998

Trade Secret Theft Crime Published Costs

It is difficult to place a value on a stolen trade secret, especially where new technology is involved. The American Society for Industrial Security (ASIS) estimates that US-based companies lose $250 million in trade secrets each year.[73] Loss estimates vary:

- The 1999 CSI / FBI survey estimates average annual loss $1.85 million per responding firm
- 1996 ASIS estimate, including traditional trade secret theft, averages $19 million

[73] ASIS, 1998

5.0 IMPACTS OF HIGH TECHNOLOGY CRIME

The impact of high technology crime includes the effects on its victims, such as the costs incurred by the public, by companies and by local, state and federal government.

Victims of High Technology Crime

There are many victims of high technology crime. Some of them are listed in Table V-1, Victims of High Technology Crime. The victims include the public, high tech corporations, other corporations, utilities and government agencies.

High technology crime is not victimless crime.

White collar crime and crimes involving access to computers and networks, and the theft of computers affect virtually all segments of society. Corporations, in general, are impacted by the theft of trade secrets and other intellectual property (IP). Other crimes affect specific segments: chip and component theft affects hardware companies; piracy and remarking software affects the software and entertainment industries, and telecommunications and cable / satellite companies are affected by the theft of communications signals.

High tech crimes are more than just direct losses -- the economy is adversely affected by firms downsizing or going out of business. As e-commerce, on-line trading and other uses of technology continue to expand, fraud will continue to expand while firms and workers from all areas will be affected.

There may also be an effect on economic development, especially if a perception that California is soft on "high technology crime" is allowed to grow.

Table V-1: Victims of High Technology Crime

Estimating the Costs of High Technology Crime

There are few statistics on the occurrence of high technology crime and none of them are universally accepted as indicating the true status of high technology crime. Nevertheless, in order to indicate the severity of the problem, an attempt has been made to estimate its cost, as shown in Appendix B: Estimating the Costs of High Technology Crime. For each type of high technology crime the table estimates:

- Revenue lost by the California private sector
- Jobs lost
- Wages lost
- State income lost
- Sales tax lost
- Local tax lost

As shown in the Appendix B, the estimated annual impacts are:

- Revenue Lost: $6,564 million
- Jobs Lost: 19,141
- Wages Lost: $923 million
- Tax Revenue Lost: $358 million

Variations of Impact

For small businesses and start-up companies, the impact of high technology crime can be more severe than for a larger company. Small businesses have very limited resources and start-up companies are often based on unique trade secrets. These types of companies can be devastated by a high technology crime.

While a certain size loss suffered by a small company could be catastrophic and hardly noticeable by a large company, the law enforcement response will be the same in each case.

A small businesses or startup company may not know how to respond to a high technology crime, since it usually would not have a security manager or access to crime-related resources.

Indications That High Technology Crime is Growing

Aside from the difficulties of measuring high technology crime directly there are indications that it is growing.

Trends in Reported Crimes

First, there are trends that this crime is growing even though certain aspects of it may decrease as a result of programs being implemented by law enforcement agencies. The CSI / FBI Computer Crime and Security surveys indicate increases in high technology crime, in most areas, for the annual surveys over the three year period of its existence.

In *Summary of Critical Statistics and Findings*[74], Mr. Vatis cites published statistics relative to computer intrusion:

- A 1998 study by the Computer Security Institute shows that 64% of the companies polled reported information system security breaches – an increase of 16% over last year. The total financial losses from the 241 organizations that could put a dollar figure on the adds up to $136,822,000. This figure represents a 36% increase in reported losses over the 1997 figure of $100,115,555..."

- "While the Carnegie Melon CERT/Coordination Center reported a small reduction in security incidents (2,134 in 1997, down from 2,573 in 1996), the type and scope of attacks indicates a disturbing increase in the use of automated scripts, enabling malevolent network users to attack very large numbers of systems with much greater efficiency."

Increase in Investigations

"…We at the FBI have seen significant increase in the number of pending computer intrusion investigations and in the number of successful prosecutions. Pending cases have in creased 133% from the beginning of FY 1997, from 206 to 480. In FY 1997, there was a 100% increase in indictments (from 10 to 21), a 950% increase in arrests (from 4 to 42), and an 88% increase in convictions (from 16 to 30).

"Although comprehensive statistics on the prevalence of identity theft are not currently available, the available data suggests that the incidence of identity theft has been increasing in recent years.

[74] Vatis, 1999, p.5

The General Accounting Office, for example, reported that consumer inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department increased from 35, 235 in 1992 to 522,922 in 1997."[75]

During the first nine months of 1998, the NIPCI (National Infrastructure Protection and Computer Intrusion) squads and teams opened 377 new cases, closed 304 cases and had a pending caseload of 526 matters. Currently there are 680 pending investigations of computer intrusion matters. The pending caseload is expected to markedly increase in the coming years."[76]

In October 1997, the FBI had fifteen pending (trade secret) investigations. As the report went to press, 37 pending theft of trade secret investigations were on the books.[77]

Increase in Training

A second indication is the increasing call for training by law enforcement officials. In one study, responses to a survey on high technology crime sent to the largest 500 police forces indicated that it was a growing threat and the most pressing need was to train police officers to handle it.[78]

Increase in Budgets to Fight High Technology Crime

A third indication is the increase in budgets to fight high technology crime by federal agencies based on their assessed needs. Among the high technology budget items for the FBI this year are increases of $58 million for networked information system and $10 million to hire and train 79 new computer forensic investigators.[79]

[75] Bernstein, 1999
[76] Vatis, 1999
[77] Gallagher, 1998
[78] Meyer, 1998
[79] Tillett, 1999

6.0 THE REGIONAL TASK FORCE EXPERIENCE

The Task Force approach is a new way to fight high technology crime. Ohlhausen points out that in order to address high technology crime adequately, California law enforcement agencies need a high level of computer knowledge, foreign language resources, assistance in tracking criminals to distant locations, the rapid flow of intelligence and certain financial and equipment resources. The best way to provide these resources is the task force approach.[80]

This approach was established with the passage of SB 1734, and the subsequent implementation of the High Technology Theft Apprehension and Prosecution Program. This program augments regional high technology crime task force programs and resources through grants administered by the Office of Criminal Justice Planning (OCJP). It also established the High Technology Crime Advisory Committee to advise OCJP on the high technology crime task forces.

California currently has three high technology task forces

- Los Angeles County and Orange County Regional High Tech Crime Task Force
- Rapid Enforcement Allied Computer Team (REACT), Silicon Valley
- Sacramento Valley Hi-Tech Crimes Task Force

It also has several more task forces in preparation. One, of note is in San Diego.

Los Angeles - Orange County High Tech Crime Task Force

While the Counties of Los Angeles and Orange have been fighting high technology crime since 1996, the Los Angeles County and Orange County Regional High Tech Crime Task Force was formed only in February 1999 after a year of planning. The two county task force serves a combined population of approximately 11,900,000.

The task force approach is believed to be the best approach to minimize multi-jurisdictional difficulties and is an effective way to prepare for the onslaught of high technology crimes saturating the region. The Los Angeles County and Orange County Regional High Tech Crime Task Force will establish and staff a computer forensics lab and training facility which will be available to non-members, caseload permitting. Certified high technology crime investigators and prosecutors will be available for consultation.

[80] Ohlhausen, 1997

The objectives of the task force are to:

- Coordinate law enforcement activities
- Pool resources and effectively share high technology investigative expertise
- Decrease high technology investigation response time
- Provide a service network to all agencies within the region
- Assess and facilitate training needs within the region
- Decrease the potential for economic loss and danger to public safety by increasing the probability of apprehension and prosecution

Related activities of the task force include:

- Provide forensic computer analysis
- Assist other member and non-member agencies
- Investigate and prosecute crimes on the Internet
- Investigate and prosecute counterfeiting / remarking of computer equipment and media
- Investigate and prosecute system intrusions, disruptions and the theft of data

Membership

The initial membership of the Task Force includes:

- Office of the Los Angeles County District Attorney
- Los Angeles County Sheriff's Department
- Long Beach Police Department
- Office of the Orange County District Attorney
- Anaheim Police Department
- Los Angeles Police Department
- Orange County Sheriff's Department
- Los Angeles County Auditor Controller
- California Department of Motor Vehicles
- California Department of Insurance

Members from the high technology industry in the region will be invited to participate

High Technology Crime in the Los Angeles County / Orange County Region

Because of the global nature of the Internet, high technology crime in the Los Angeles County / Orange County area mirrors the crime problem of the entire state: fraud, computer intrusions, consumer protection violations, sexual molestation of children, stalking, trademark violation, stock market manipulation, identity theft, banking manipulation, and credit manipulation have been examined as problems in the region. In addition, theft of components, remarking of high technology goods and counterfeiting have been previously investigated and prosecuted by the members of the task force.

Based on a quick survey of two thirds of the law enforcement agencies in both counties, 3,238 high technology crime investigations were reported for the calendar year 1998. These numbers are reported to be growing.

Since January 1996, the Los Angeles District Attorney's Office has prosecuted over 269 defendants for computer hacking with over half convicted. During the same period the Los Angeles District Attorney prosecuted over 1,942 defendants for telecommunications fraud with most having been convicted.

Due to the recent formation of the task force, data is not available for other types of high technology crimes -- that is the high technology crime could not be separated from conventional forms of fraud and other crimes. Also, amounts of restitution have not been tracked, although in one case, alone, the defendants convicted of telecommunications fraud were ordered to pay over $700,000 to cellular providers.

Detailed statistics for the Los Angeles County and Orange County Regional High Tech Crime Task Force are attached.

Rapid Enforcement Allied Computer Team (Silicon Valley)

The Rapid Enforcement Allied Computer Team (REACT) is a multi-jurisdictional High Technology Crime Task Force targeting high technology crimes in southern Alameda County, Santa Clara County and Santa Cruz County. Formed in April 1997, the task force serves a region of approximately 2,000,000 persons.

The objectives of the task force are to:

- Expand and improve the investigation, deterrence and prosecution of systemic high technology crime
- Identify locations used in connection with technology theft offenses
- Identify local trends and patterns of high technology crime
- Increase the recovery rate of stolen computer components

- Provide law enforcement agencies information, expertise, support and coordination of high technology theft investigations
- Seek input and solicit cooperation from the private sector to promote public awareness

The members of the task force are:

- Alameda County District Attorney's Office
- California State Department of Justice
- City of San Jose
- Federal Bureau of Investigation
- Fremont Police Department
- Internal Revenue Service
- Milpitas Police Department
- Mountain View Police Department
- Santa Clara County District Attorney's Office
- Santa Clara County Sheriff's Department
- Santa Clara (City) Police Department
- Santa Cruz County District Attorney's Office
- Secret Service
- Sunnyvale Police Department

The task force also has a close working relationship with the San Jose Police Department's High Tech Crime Squad and the FBI High Tech Crime Unit.

<u>High Technology Crime in the Silicon Valley Region</u>

A significant increase in high technology cases such as gray market activities, remarking of CPUs, employee theft, cargo theft and Internet fraud is evident in the REACT area. Over the last 29 months REACT has investigated or assisted with 170 high technology cases which has resulted in 122 arrests and 115 search warrants being served. The total monetary loss suffered by the 229 victims of these cases was $39.1 million, of which $23.9 million occurred in the last 12 months.

Of the 170 cases can be broken down as follows:

- 7 - white collar crime
- 8 - unlawful computer and network access
- 2 - money laundering
- 1 - telephone services theft
- 4 - software piracy
- 99 - theft of computer components and other high technology products
- 27 - remarking (20 hardware; 7 software)
- 10 - theft of trade secrets
- 12 - others

Detailed statistics for REACT are attached.

Sacramento Valley Hi-Tech Crimes Task Force

The Sacramento Valley Hi-Tech Crimes Task Force was created in December of 1995 for the purpose of conducting multi-jurisdictional investigations that track and disrupt the illicit commerce of stolen goods, investigates and prosecutes suspects engaged in white collar crime, organized crime and fraud. The task force serves a four county region with a combined population of approximately 1,700,000.

The Sacramento Valley Hi-Tech Crimes Task Force conducts multi-jurisdictional investigations, tracks and disrupts the illicit commerce of stolen high tech goods and investigates and prosecutes suspects engaged in a variety of economic and organized crime. The task force provides technical support and computer forensic examinations for Northern California jurisdictions that do not have the necessary resources or expertise. The task force also provides training to line officers and investigators throughout Northern California.

The objectives of the task force are to:

- Identify, investigate and prosecute high technology crime cases
- Increase investigator time
- Increase and upgrade the computer lab
- Provide sophisticated computer forensic examinations as required
- Enhance the intelligence infrastructure to develop information on systemic high technology crime
- Provide training to member agencies and others, as available
- Support legislation

The membership of the task force is comprised of the:

- California Department of Justice
- California Highway Patrol
- El Dorado County Sheriff's Department
- Federal Bureau of Investigation
- Folsom Police Department
- Placer County District Attorney's Office
- Placer County Sheriff's Department
- Roseville Police Department
- Sacramento County District Attorney's Office
- Sacramento County Probation Department
- United States Attorney's Office
- West Sacramento Police Department
- Yolo County District Attorney's Office

The private sector members of the Advisory Steering Committee include:

- Airtouch Cellular
- Apple Computer
- AT&T Wireless
- Comcast
- Hewlett-Packard
- Intel
- NEC
- Packard Bell

High Technology Crime in the Sacramento Valley Region

The task force investigates thefts of computers and components, on-line crimes and telecommunications fraud. The task force investigated 178 cases during its first year of operation in 1996, 283 cases in 1997 and 285 cases in 1998. The dollar amount of recovered property was $9.1 million in 1996, $411,000 in 1997 and $1.2 million in 1998.

The case breakdown for 1998 was 16 white collar (financial fraud), 38 computer and network-related crimes, 4 telecommunications fraud, 7 cable theft, 70 computer and component thefts and 31 other high technology crimes. In addition, the task force conducted 113 forensic examinations. Detailed statistics for the Sacramento Valley Hi-Tech Crimes Task Force are attached.

New Task Forces

San Diego

The District Attorney's Office of San Diego County is leading a grass roots effort to establish a high technology crime task force in the San Diego region. They are in the process of contacting local agencies who may become participants - both inside and outside the county and federal and state agencies. They are also setting up meetings with security representatives from some of the larger high tech companies. They expect to formalize agreements in the coming months.

Also the county is working with the FBI to set up a jointly operated forensics lab. Eight examiners who will work in the lab just completed advanced training and the founding agencies have made a two year minimum commitment. The FBI has provided a lab site at no cost for five years.

Concerning types of crime, the region has also been the victim of violent takeover robberies where the target is computer components. A link between street gangs and computer thefts has been observed. Also the private sector is reported to be reluctant to report internal thefts, even when the losses are in the hundreds of thousands of dollars or more. When there is a task force, where highly trained law enforcement can investigate and prosecute, corporate victims are more willing to report high technology crimes.

7.0 HIGH TECHNOLOGY THEFT APPREHENSION AND PROSECUTION STRATEGY

In order to further develop a program to effectively fight high technology crime in California, a strategy has been developed that takes into account the different types and extent of high technology crime, including the differences between regions, and local needs and programs. The infrastructure systems that support high technology crime, such as the "gray market" will be placed under attack so that high technology criminals will have no potential benefit from their crime and that the property that is stolen or used in the crime can be recovered.

The strategy, to be implemented through regional task forces, identifies priorities for law enforcement, including:

- To apprehend and prosecute criminal organizations, networks, and groups of individuals engaged in the following activities:
  - Theft of computer components and other high technology products.
  - Violations of PC Sections 211, 350, 351a, 459, 496, 537e, 593d, and 593e.
  - Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.
  - Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.
  - Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.

- To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

- To apprehend and prosecute individuals and groups engaged in the theft of intellectual property and trade secrets.

- To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.

Objectives

The legislation that created the High Technology Theft Apprehension and Prosecution Program and the High Technology Crime Advisory Committee requires that a strategy be developed to combat high technology crime. The strategy is intended to be a roadmap for use by regional high technology task forces in accomplishing their mission of reducing the impact of high tech crime on the citizens, industries, and governments of the State of California. The objectives of these regional task forces are threefold:

Identify "systemic high technology crime" in its region. That term refers to the criminal activities of individuals who, acting alone or in concert, provide an infrastructure which makes particular high technology crimes profitable.

For example, the large-scale theft of components could not exist without a portion of the "gray market" knowingly purchasing and reselling stolen components. Similarly, software, cable, and video piracy depend upon distribution networks for counterfeit goods. Telecommunications fraud depends upon markets for stolen access codes, and so on.

Gather and analyze information to determine the key individuals responsible for the maintenance of that "system", both within and outside of the region.

Use the gathered intelligence to build and prosecute cases against those individuals in conjunction with other agencies, including state and federal agencies. Task forces are expected to pursue cases outside of its region where necessary; the ability of the task force to create effective partnerships with other agencies and task forces will be vital.

Implementation

The formation of the task force and the membership is only restricted by the language of the legislation which requires that law enforcement and prosecutors from at least two counties participate as well as a representative of State law enforcement. Memorandum of agreement and other administrative necessities are left to the task force to accomplish. The involvement of federal law enforcement agencies including the FBI, Secret Service, IRS and Customs at some level will be required for success by each regional task force. The aggressive recruitment of members of these agencies by the regional task forces is strongly encouraged and will be carefully reviewed during future funding cycles.

The participating agencies must create a Regional Task Force Advisory Committee. Cooperation between the task forces and the private sector industry is critical to success. The committee must be composed of command level officers from the participating agencies and members of prominent industries victimized by high technology crime in the region. The number of members on the committee and the process for selecting members will vary by region and the crime environment within that region. As discussed later in the mission statement, the role of the advisory committee is significant and great care should be given to its creation. The Advisory Committee will be responsible for the formulation and execution of the regional strategy and for monitoring and reporting on the activities of the task force. The industry representatives should have sufficient stature within their firms to commit resources if required.

Mission

Each task force must identify the most serious systemic high technology crime(s) in its region. Advisory Committees are critical to this process because they include representatives from local high technology industries that are typically victims of high technology crime.

Each Advisory Committee is charged with:

- collecting loss data from companies represented on the Committee
- collecting loss data from other businesses and public institutions within the region
- ascertaining whether local criminals are responsible for significant losses elsewhere in California
- Interpreting loss data to determine which systemic high technology crimes committed within the region are causing the most harm

The unwillingness of victims to report losses has led the public to underestimate the impact of high technology crime and made it difficult for law enforcement agencies to determine which crimes are most serious. Thus, it is imperative that private sector Advisory Committee members collect and share loss data. Companies seeking anonymity may present data to a public sector member of the committee for aggregation with other data. Non-member businesses will also contribute valuable data; committees should consider surveying local industry associations and individual companies. Public institutions, such as schools and universities, may also provide important information.

However, confining the inquiry to one region may not be sufficient. A striking feature of high technology crime is that crimes committed in one jurisdiction often affect victims elsewhere. For example, although most victims of software piracy are headquartered in Northern California, many pirates manufacture and distribute packaging and other materials in Southern California.

Thus, committees should survey other task forces to assess whether local criminals are committing "multi-jurisdictional" crimes.

Finally, each committee must interpret the data and target one or more systemic high technology crimes. Criteria for selection includes, but are not limited to:

- the economic loss attributable to each high technology crime
- the degree to which a particular high technology crime is likely to grow in importance in the near future
- actual or potential personal injury attributable to each crime

Economic loss includes direct and indirect loss, such as the value of items stolen or counterfeited, lost business opportunities (e.g., due to theft of inventory), and expenses involved in repairing damage and enhancing security. Although most high technology crime does not result in personal injury, a few crimes do carry that potential, including armed robberies of components, child pornography and seduction of children via the Internet, and computer intrusion directed at critical infrastructure (e.g., hospitals, utilities).

Finally, Advisory Committees can help identify threats on the horizon. Although task forces will generally focus on crimes causing the most damage, occasionally a new crime or group of criminals will pose such an urgent threat that task forces must respond immediately.

Establishing the Intelligence Process

The collection of information by Regional Task Forces will be critical to the success of the efforts on both a regional and state-wide basis. Each task force will be required to collect and maintain certain types of information on a common basis for inclusion in the database developed in cooperation with the California Department of Justice (DOJ) as part of this legislative mandate. When this database/intelligence system is in place, all task forces will be required to participate and can benefit from the data collection and analysis. The basic information types that must be collected are:

The Offense File will be part of each task force's records system. The file will include TF case number, handling agency case number, assigned investigator, date and time of offense, suspect information, victim information, verified loss, case status and a brief summary of the case.

The Suspect File will come from offense reports, arrest reports and field interview reports and will identify arrestees, suspects and known associates who have come to the attention of the task force. Data will include name, date of birth, identifying numbers (CDL, CII, FBI, PFN, etc.), specific descriptors (tattoos, scars, etc.,) associated businesses, corresponding case numbers and known associates.

The Property File will include losses, recoveries, and type of property, etc.; this file will not only provide valuable shared intelligence but also document the effectiveness of the task force efforts and quantify the scope of the high tech crime in a given area.

Modus Operandi information must be kept in a manner that will allow task force members to share the information with other members, other task forces and law enforcement involved in similar cases.

Information collected, stored and analyzed in the DOJ system will be available to law enforcement members of the regional task forces and other law enforcement as needed.

Attacking the Infrastructure

Task forces will attack the infrastructure underlying one or more high technology crimes by targeting the individuals and businesses operating that infrastructure. These operations may require significant time and resources; they may also require travel to other regions and assistance from other law enforcement agencies. The hallmark of the task force approach is to follow the case wherever it leads, and to enlist the support of every local, state, and federal agency with the jurisdiction and tools to pursue the investigation.

The measuring stick for success is not the number of investigations or prosecutions conducted by a task force, but the damage it inflicts on the infrastructure. Although measuring that damage with precision is difficult, indicators of success may include:

- a decrease in the number of establishments associated with distributing and/or selling goods similar to those stolen or counterfeited in the past
- seizures and forfeitures of equipment used to commit high technology crime (e.g., equipment used to counterfeit CD-ROMs, clone cell phones, or produce counterfeit cable TV hardware)
- conviction and incarceration of multiple defendants, with one or more defendants sentenced to long state or federal prison terms
- a decrease in the incidence of the targeted high technology crime within the region.

For high technology crimes involving the theft and resale of stolen property, a striking indicator of success is a shrinkage in the secondary market associated with that property. For example, a sudden shortage in components or purchases through legitimate channels by businesses which did not use those channels previously may indicate damage to the infrastructure which formerly supplied those components.

A more visible indicator of success is the seizure and forfeiture of part or all of the infrastructure. Task forces are encouraged to use the tools available under state and federal law to "follow (and take) the money."

Another visible indicator is the incapacitation of the criminal enterprise by imprisonment of its leaders. Task forces should aim to do more than "roll up" foot soldiers, although pursuing such people may yield valuable intelligence and evidence. Rather, the aim is to build substantial cases against the ringleaders and put them in prison.

Finally, the ultimate goal of any attack on the infrastructure is to reduce the incidence of high technology crime supported by that infrastructure. For example, armed robberies in the Silicon Valley fell more than five-fold after a joint local-federal investigation several years ago.

However, these indicators are not precise; nor are they intended as rigid guidelines. In many cases there will be no data available concerning the incidence of a particular high technology crime, making "before and after" comparisons impossible. Anecdotal evidence of effectiveness by Advisory Committee members may be the only evidence available. Other measures of effectiveness may prove equally elusive. Forfeiture is not possible in every case; some courts are unwilling to punish any economic crime severely.

The aim of this strategy is to move law enforcement away from the traditional approach of opening and closing large numbers of unrelated cases, and toward a cohesive plan of attacking high technology crime systematically. Task forces should emphasize quality over quantity, and focus on disabling the infrastructure which makes high technology crime profitable.

Ancillary Duties

While it is clear that the purpose of this strategy is to focus on a limited number of crime systems and realize long-term significant reductions in those systems, we realize that the task forces must also work other cases that arise within their region. The legislation defines the types of penal code violations that qualify as high tech crimes and it is the intent of the law that regional task forces will lead in the investigation of these offenses. The process for selecting and responding to other offenses will be the responsibility of the task force commander with advice from the regional advisory committee. The goal should be to work those offenses which will have a

significant positive effect on the local communities and the state without trying to "make the numbers". While there will be some requirement for the task force members to conduct forensic computer examinations, this should not be a key or regular task. Every effort should be made to focus the task force members on their investigative tasks while shielding them from "high tech" tasks handed off to the group by departments in the region. The measurement system will clearly reward those who focus on the strategic goals and not those who are building big numbers.

Training

Task Force Members

Training is a key element of this strategy and we recognize that more than normal training will be required for task force members. These training requirements will include:

- OCJP specific requirements for managing projects including fiscal procedures and other administrative rules and processes.
- DOJ sponsored training on Criminal intelligence fundamentals, Intelligence information analysis, and link analysis.
- Other coursework on basic and expanded crime analysis, asset forfeiture procedures and undercover and sting operations as required.

Private industry training on product security measures in use within the region. This would include product design and markings that would serve to identify and locate certain products such as lot numbers, serial numbers, holograms and other security techniques. This education will be critical to the investigation of certain acts like possession of stolen property, counterfeiting of product or piracy in its various forms.

Patrol Officers And Criminal Investigators

The task forces should train patrol and investigative personnel in the regional agencies to increase the effectiveness of patrol operations and investigation by:

- Communicate with patrol officers and investigators wherever possible to inform them of the type of information required by task force investigators at the outset to initiate and successfully investigate and prosecute high tech crimes.
- Create roll-call training sessions to include topics such as counterfeit product recognition, M.O. tendencies of identified offenders, evidence collection and search

warrant protocol in high tech cases, etc. This training will require the close cooperation of the local agencies and will require a time commitment from the task force.

The task forces should establish an on-call system to make task force investigators available to respond to inquiries by patrol officers and criminal investigators. Timely response to questions regarding high tech cases, investigations and evidence collection will allow task force members to judge incidents as they happen and give them the opportunity to take on new major cases, or to interview subjects quickly. The availability of the high tech task force on-call member needs to be widely known to the agencies within the region.

High Tech Companies / Private Industry

The regional advisory committee should take the lead in creating an effective relationship with the private sector in order to assure that each other understand the needs of the law enforcement community and the private sector. This relationship should facilitate the training of employees of the high tech industries as well as other companies in the region who are targeted.

Based upon information learned from investigations, the task force should train private sector companies on appropriate “target hardening”.

Private sector companies should be trained on the requirements for a successful investigation and what they need to do to facilitate the task forces work.

Assist high tech companies in reviewing security processes that have been compromised in past incidents and recommending appropriate fixes.

8.0 THE POTENTIAL OF A HIGH TECHNOLOGY CRIME DATEBASE SYSTEM

The availability of a High Technology Crime Database System will greatly assist local law enforcement agencies in the fight against high technology crime. As noted above, some high technology crime is likely to be multi-jurisdictional, committed by organized groups, and have other complicating attributes. As discussed in the following sections about legislative mandate, purpose, content and functionality, the database system will greatly aid in the investigation of high technology crimes.

Legislative Mandate

The passage of SB 1734 also provided funding for a high technology crime database. The law currently stipulates that "up to 10% of funds (appropriated into the High Technology Theft Apprehension and Prosecution Program Trust Fund) shall be used for developing and maintaining a state-wide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies" [Sec. 13848.4(c) of the California Penal Code]." This funding will provide assistance to the database program as long as the High Technology Task Forces are funded.

Purpose

The overall purpose of the High Technology Crime Database System, stated above, is to develop and distribute intelligence information to participating agencies. This includes:

- The identification and collection of needed information
- The capability to enter, process and output the needed information
- The software, hardware and data communications components required for the operation of the system
- The capability to share information between jurisdictions, task forces, and state and federal entities
- The capability to provide access security and to protect against unwanted intruders

In the interviews, it was seen that the information was usually collected, but was not readily accessible to the investigating officer. Often, information in other jurisdictions could only be

accessed through personal contact. The database will fill a need to share information about these types of crimes.

Content

The database will be intelligence-based and will have information on cases, including suspects, the type and approach to the crime and other relevant information. Information on cases will result from formal investigations. Other information on suspicious incidents will also be available in the database, but may not initially be linked to a particular case.

The types of crime to be identified in the database include:

- Computer / component theft
- Intellectual property theft (including trade secrets)
- Computer / network intrusion
- Computer-assisted crime (various types of fraud, use of stolen credit cards, stolen identity, cyber-stalking)
- Software piracy
- Entertainment industry piracy (e.g. Movies, video, music, games)
- Cable / satellite TV signal theft
- Telecommunications services theft
- Other (e.g. Child pornography, links to other types of crime, etc.)

Functionality

The database should support a logical approach to the investigation of high technology crime, including the ability to correlate information with other task forces, including those working on hijackings, gangs or drugs. The database should also be useful to investigators working on other types of crime who suspect a possible link to high technology crime.

> *The high technology crime database will be extremely useful. In addition to sharing information between regions within the state, information will be shared with other states, with federal entities and with other countries.*

Information from the database may eventually be available to local patrol units contingent on security provisions and cost considerations.

9.0 CONCLUSIONS

High technology crime in California is a significant societal problem that is not well understood. Every interview conducted for this report and virtually every source of information uncovered on the subject implies that its level is high and is growing rapidly. The only indication that high tech crime dropped occurred when a task force targeted a particular type of crime and caused those criminals, not arrested, to focus their efforts in other jurisdictions or on other types of crime.

An argument can also be made that high technology crime is growing because there is:

- An increase in reported high technology crime
- An increase in investigations of high technology crime
- An increase in training on high technology crime
- An increase in budgets to fight high technology crime

This report presents a strategy to fight high technology crime. The strategy addresses several issues and is the result of a continuing program by State Government to fight high technology crime. In an era where programs continue to compete for scarce resources it is difficult to emphasize a program lacking background information. That's why the state's approach must be two-fold: fighting high technology crime in cost-effective ways, and collecting and disseminating information about high technology crime.

Lack of Accurate Information

For various reasons there is insufficient data about high technology crime. Most of what is known is anecdotal; the rest is based on surveys which have readily admitted biases.[81] To our knowledge there are no scientific surveys and no programs at universities or research institutes that publish information about high technology crime on a routine basis.

There is a reticence among the private sector to share information about high technology crime. Among manufacturers, this reluctance may be overcome by the realization that it happens to everyone and doesn't usually affect the public image of the company. Assisting in this realization will be the efforts of insurance companies to require safeguards and the further realization by the companies that the least expensive approach to resolving the problem will be actively fighting high technology crime.

[81] For example, the CSI / FBI survey is sent only to CSI members who, presumably, are interested and knowledgeable about the high tech crime. When interpreting its results, one begins to wonder about the difficulties of other managers who may not be interested or knowledgeable about the subject.

For service companies, however, the problem is real. The perception that an organization such as an on-line bank or an electronic commerce site is susceptible to high technology crime may lead to a real impact on its bottom line. In this case there is a need for secrecy when a company cooperates with an investigating law enforcement agency.

> *Legislation is needed to restrict certain high tech criminal data from becoming public information. This is the only way we will ever have a clear picture of this rapidly growing area of crime.*

Increasing levels of computer and Internet-related crime will embroil law enforcement is issues of privacy. The state should play a leading role in analyzing and informing law enforcement officials about privacy, disclosure and related issues, especially as they relate to high technology crime.

> *Privacy is a big issue but legislation is needed to address the use of computer "fingerprints", use of personal data in on-line activity and other related issues.*

Participation in the High Technology Theft Apprehension and Prosecution Program will require the High Technology Crime Task Forces to collect and submit data to the state on an annual basis. This is a beginning of a programmatic effort to collect the required information. But more is needed - information about high technology crime should become part of the routine data collected about every crime. But in order for this to happen there will need to be agreement among national, state and local law enforcement organizations on the types and definitions of high technology crime.

> *The Uniform Crime Report should have at least a high technology crime "block" to check in order to begin to generate information on these crimes. According to one source this would take "millions" of dollars and so the suggestion has not been seriously considered.*

Currently, information about crimes in other non-local jurisdictions is available only by person-to-person contact. Information about suspicious activity may not be available at all. These problems will be addressed by a high technology crime database system that will be implemented over the next year. The system will become more useful as it makes an increasing number of incidents and crimes available to the scrutiny of investigators, state-wide.

Jurisdiction and Prosecution

Issues of jurisdiction threaten to have a major impact on the pursuit of high technology criminals. Many types of high technology crime are independent of location -- that is a local victim may fall prey to a criminal located anywhere in the world! And crimes that cross jurisdictions are usually not prosecuted by local agencies, an increasingly common situation that guides the activities of local law enforcement agencies according to federal objectives and budgets rather than the concerns of the local community.

> *Jurisdiction is a major issue! Laws do not adequately address which agency will address crimes committed by a computer criminal in Los Angeles on an internet business transaction in Denver. Or Tokyo. Joint jurisdiction is probably the most logical approach, but it requires clear definition in legislation.*

> *Jurisdiction is a key issue but could be resolved with legislation dealing with cooperation among law enforcement agencies, including the requirement that an evaluation be made as to which agency has the best case and other decision elements.*

High Technology Theft Apprehension and Prosecution Strategy

A strategy to fight high technology crime has been developed as part of the High Technology Theft Apprehension and Prosecution Program by the High Technology Crime Advisory Committee. The strategy has a grass-roots basis. Each task force must identify the most serious systemic high technology crime(s) in its region. Regional Advisory Committees are critical to this process because they include representatives from local high technology industries that are typically victims of high technology crime.

Task forces will attack the infrastructure underlying one or more high technology crimes by targeting the individuals and businesses operating that infrastructure and to reduce the incidence of high technology crime supported by that infrastructure. The aim of this strategy is to move law enforcement away from the traditional approach of opening and closing large numbers of unrelated cases, and toward a cohesive plan of attacking high technology crime systematically. Task forces should emphasize quality over quantity, and focus on disabling the infrastructure which makes high technology crime profitable.

Training is a key element of this strategy and we recognize that more than normal training will be required for task force members. The task forces should train patrol and investigative personnel in the regional agencies to increase the effectiveness of patrol operations and investigation.

Technical Assistance

Organizations like the National Law Enforcement and Corrections Technology Center Western Region (NLECTC-West) are available to provide technical assistance to task forces and police departments fighting high technology crime. In concert with the National Institute of Justice Office of Science and Technology (NIJ/OST), NLECTC-West provides research, review, development, and implementation innovative technology for both regional and National law enforcement and corrections services. It is the goal of NLECTC-West to put needed, affordable, and workable technology into the hands of front line law enforcement and corrections officers so they can do a better job of protecting our citizens.

SB 1734 High-tech crimes.

BILL NUMBER: SB 1734 ENROLLED 08/18/98

PASSED THE SENATE AUGUST 18, 1998
PASSED THE ASSEMBLY AUGUST 13, 1998
AMENDED IN ASSEMBLY JULY 2, 1998
AMENDED IN ASSEMBLY JUNE 11, 1998
AMENDED IN SENATE APRIL 22, 1998
AMENDED IN SENATE APRIL 2, 1998

INTRODUCED BY Senator Johnston
FEBRUARY 18, 1998

An act to amend Sections 502.01, 13848, 13848.2, 13848.4, and 13848.6 of the Penal Code, relating to computer crimes, and declaring the urgency thereof, to take effect immediately.

LEGISLATIVE COUNSEL'S DIGEST

SB 1734, Johnston. High-tech crimes.

(1) Existing law provides for the forfeiture of certain electronic equipment upon a judicial finding that this equipment was used in the commission of specified crimes.

This bill would clarify that these provisions also apply to "illegal telecommunications equipment" by correcting an erroneous cross-reference.

(2) Existing law states the intent of the Legislature to provide local law enforcement with the tools necessary to interdict high technology crimes. In this connection, existing law defines an enumerated list of offenses as high technology crimes. Funds from a specified program within the Office of Criminal Justice Planning are to be expended for the interdiction of these crimes.

This bill would recast these provisions by providing that the executive director may define additional high technology crimes, and by revising the enumerated list to include crimes involving the theft of access or trade secrets.

(3) Existing law authorizes the Executive Director of the Office of Criminal Justice Planning, in consultation with the High Technology Steering Committee, to allocate and award funds to counties with high technology theft crime units upon application by local district attorneys and sheriffs and upon approval by the board of supervisors of the county.

This bill would instead provide that the executive director shall award these funds to regional high technology theft crime programs. The bill would also allow chiefs of police to apply for this assistance, upon approval by the board of supervisors of the participating county.

(4) Existing law provides that, upon appropriation by the Legislature, 10% of the funds deposited into the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be used for developing and maintaining a statewide data base on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies.

This bill would instead provide that up to 10% of moneys appropriated into this fund may be used for that purpose.

(5) Existing law establishes the High Technology Steering Committee, the membership of which is comprised of 4 industry representatives, and one representative of local law enforcement from each area in which a regional task force will be situated.

This bill would rename this committee as the High Technology Crime Advisory Committee, expand its membership to 15 individuals designated by specified law enforcement and industry associations, provide that the chair of the committee is to be designated by the Executive Director of the Office of Criminal Justice Planning, impose certain attendance and notice requirements, and provide for the creation of subcommittees. This bill would require the committee to prepare a comprehensive written strategy to accomplish specified goals, and to annually review the effectiveness of the regional task forces and provide its findings in a report to the Legislature and the Governor.

(6) This bill would declare it is to take effect immediately as an urgency statute.

SECTION 1. Section 502.01 of the Penal Code is amended to read:

502.01. (a) As used in this section:

(1) "Property subject to forfeiture" means any property of the defendant that is illegal telecommunications equipment as defined in subdivision (g) of Section 502.8, or a computer, computer system, or computer network, and any software or data residing thereon, if the telecommunications device, computer, computer system, or computer network was used in committing a violation of subdivision (c) of Section 502 or Section 502.7 or 502.8, or was used as a repository for the storage of software or data obtained in violation of those provisions. If the defendant is a minor, it also includes property of the parent or guardian of the defendant.

(2) "Sentencing court" means the court sentencing a person found guilty of violating subdivision (c) of Section 502 or Section 502.7 or 502.8, or, in the case of a minor found to be a person described in Section 602 of the Welfare and Institutions Code because of a violation of those provisions, the juvenile court.

(3) "Interest" means any property interest in the property subject to forfeiture.

(4) "Security interest" means an interest that is a lien, mortgage, security interest, or interest under a conditional sales contract.

(5) "Value" has the following meanings:

(A) When counterfeit items of computer software are manufactured or possessed for sale, the "value" of those items shall be equivalent to the retail price or fair market price of the true items that are counterfeited.

(B) When counterfeited but unassembled components of computer software packages are recovered, including, but not limited to, counterfeited computer diskettes, instruction manuals, or licensing envelopes, the "value" of those components of computer software packages shall be equivalent to the retail price or fair market price of the number of completed computer software packages that could have been made from those components.

(b) The sentencing court shall, upon petition by the prosecuting attorney, at any time following sentencing, or by agreement of all parties, at the time of sentencing, conduct a hearing to determine whether any property or property interest is subject to forfeiture under this section. At the forfeiture hearing, the prosecuting attorney shall have the burden of establishing, by a preponderance of the evidence, that the property or property interests are subject to forfeiture. The prosecuting attorney may retain seized property that may be subject to forfeiture until the sentencing hearing.

(c) Prior to the commencement of a forfeiture proceeding, the law enforcement agency seizing the property subject to forfeiture shall make an investigation as to any person other than the defendant who may have an interest in it. At least 30 days before the hearing to determine whether the property should be forfeited, the prosecuting agency shall send notice of the hearing to any person who may have an interest in the property that arose before the seizure.

A person claiming an interest in the property shall file a motion for the redemption of that interest at least 10 days before the hearing on forfeiture, and shall send a copy of the motion to the prosecuting agency and to the probation department.

If a motion to redeem an interest has been filed, the sentencing court shall hold a hearing to identify all persons who possess valid interests in the property. No person shall hold a valid interest in the property if, by a preponderance of the evidence, the prosecuting agency shows that the person knew or should have known that the property was being used in violation of subdivision (c) of Section 502 or Section 502.7 or 502.8, and that the person did not take reasonable steps to prevent that use, or if the interest is a security interest, the person knew or should have known at the time that the security interest was created that the property would be used for a violation.

(d) If the sentencing court finds that a person holds a valid interest in the property, the following provisions shall apply:

(1) The court shall determine the value of the property.

(2) The court shall determine the value of each valid interest in the property.

(3) If the value of the property is greater than the value of the interest, the holder of the interest shall be entitled to ownership of the property upon paying the court the difference between the value of the property and the value of the valid interest.

If the holder of the interest declines to pay the amount determined under paragraph (2), the court may order the property sold and designate the prosecutor or any other agency to sell the property. The designated agency shall be entitled to seize the property and the holder of the interest shall forward any documentation underlying the interest, including any ownership certificates for that property, to the designated agency. The designated agency shall sell the property and pay the owner of the interest the proceeds, up to the value of that interest.

(4) If the value of the property is less than the value of the interest, the designated agency shall sell the property and pay the owner of the interest the proceeds, up to the value of that interest.
(e) If the defendant was a minor at the time of the offense, this subdivision shall apply to property subject to forfeiture that is the property of the parent or guardian of the minor.
(1) The prosecuting agency shall notify the parent or guardian of the forfeiture hearing at least 30 days before the date set for the hearing.

(2) The computer or telecommunications device shall not be subject to forfeiture if the parent or guardian files a signed statement with the court at least 10 days before the date set for the hearing that the minor shall not have access to any computer or telecommunications device owned by the parent or guardian for two years after the date on which the minor is sentenced.

(3) If the minor is convicted of a violation of subdivision (c) of Section 502 or Section 502.7 or 502.8 within two years after the date on which the minor is sentenced, and the violation involves a computer or telecommunications device owned by the parent or guardian, the original property subject to forfeiture, and the property involved in the new offense, shall be subject to forfeiture notwithstanding paragraph (2).

(f) If the defendant is found to have the only valid interest in the property subject to forfeiture, it shall be distributed as follows:

(1) First, to the victim, if the victim elects to take the property as full or partial restitution for injury, victim expenditures, or compensatory damages, as defined in paragraph (1) of subdivision (e) of Section 502. If the victim elects to receive the property under this paragraph, the value of the property shall be determined by the court and that amount shall be credited against the restitution owed by the defendant. The victim shall not be penalized for electing not to accept the forfeited property in lieu of full or partial restitution.

(2) Second, at the discretion of the court, to one or more of the following agencies or entities:

(A) The prosecuting agency.

(B) The public entity of which the prosecuting agency is a part.

(C) The public entity whose officers or employees conducted the investigation resulting in forfeiture.

(D) Other state and local public entities, including school districts.

(E) Nonprofit charitable organizations.

(g) If the property is to be sold, the court may designate the prosecuting agency or any other agency to sell the property at auction. The proceeds of the sale shall be distributed by the court as follows:

(1) To the bona fide or innocent purchaser or encumbrancer, conditional sales vendor, or mortgagee of the property up to the amount of his or her interest in the property, if the court orders a distribution to that person.

(2) The balance, if any, to be retained by the court, subject to the provisions for distribution under subdivision (f).

SEC. 2. Section 13848 of the Penal Code is amended to read:

13848. (a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

(b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

(1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.

(2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers and networks.

(3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.

(4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.

(5) Software piracy and other unlawful duplication of information.

(6) Theft and resale of computer components and other high technology products produced by the high technology industry.
(7) Remarking and counterfeiting of computer hardware and software.

(8) Theft of trade secrets.
(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

SEC. 3. Section 13848.2 of the Penal Code is amended to read:

13848.2. (a) There is hereby established in the Office of Criminal Justice Planning a program of financial and technical assistance for law enforcement and district attorneys' offices, designated the High Technology Theft Apprehension and Prosecution Program. All funds appropriated to the Office of Criminal Justice Planning for the purposes of this chapter shall be administered and disbursed by the executive director of the office in consultation with the High Technology Crime Advisory Committee as established in Section 13848.6 and shall to the extent feasible be coordinated with federal funds and private grants or private donations that are made available for these purposes.

(b) The Executive Director of the Office of Criminal Justice Planning is authorized to allocate and award funds to regional high technology crime programs which are established in compliance with Section 13848.4.

(c) The allocation and award of funds under this chapter shall be made on application executed by the district attorney, county sheriff, or chief of police and approved by the board of supervisors for each county that is a participant of a high technology theft apprehension and prosecution unit.

(d) In identifying program areas that will be eligible for competitive application during the 1998-99 fiscal year for federal funding pursuant to the Edward Byrne Memorial State and Local Law Enforcement Assistance Programs (Subchapter V (commencing with Section 3750) of Chapter 46 of the United States Code), the Office of Criminal Justice Planning shall include, to the extent possible, an emphasis on high technology crime by selecting funding areas that would further the use of federal funds to address high technology crime and facilitate the establishment of high technology multijurisdictional task forces.

(e) The Office of Criminal Justice Planning shall allocate any increase in federal funding pursuant to the Anti-Drug Abuse Act (Public Law 100-690) for the 1998-99 fiscal year to those programs described in subdivision (d).

SEC. 4. Section 13848.4 of the Penal Code is amended to read:

13848.4. (a) All funds appropriated to the Office of Criminal Justice Planning for the purposes of this chapter shall be deposited in the High Technology Theft Apprehension and Prosecution Program Trust Fund, which is hereby established. The fund shall be under the direction and control of the executive director. Moneys in the fund, upon appropriation by the Legislature, shall be expended to implement this chapter.

(b) Moneys in the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement and prosecutors to deter, investigate, and prosecute high technology-related crimes. After deduction of the actual and necessary administrative costs referred to in subdivision (f), the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement, state police, and local prosecutors to deter, investigate, and prosecute high technology-related crimes. Any funds distributed under this chapter shall be expended for the exclusive purpose of deterring, investigating, and prosecuting high technology-related crimes.

(c) Up to 10 percent of the funds shall be used for developing and maintaining a statewide data base on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies. Any funds not expended in a fiscal year for these purposes shall be distributed to regional high technology theft task forces pursuant to subdivision (b).

(d) Any regional task force receiving funds under this section may elect to have the Department of Justice administer the regional task force program. The department may be reimbursed for any expenditures incurred for administering a regional task force from funds given to local law enforcement pursuant to subdivision (b).

(e) The Office of Criminal Justice Planning shall distribute funds in the High Technology Theft Apprehension and Prosecution Program Trust Fund to eligible agencies pursuant to subdivision (b) in consultation with the High Technology Crime Advisory Committee established pursuant to Section 13848.6.

(f) Administration of the overall program and the evaluation and monitoring of all grants made pursuant to this chapter shall be performed by the Office of Criminal Justice Planning, provided that funds expended for these functions shall not exceed 5 percent of the total amount made available under this chapter.

SEC. 5. Section 13848.6 of the Penal Code is amended to read:

13848.6. (a) The High Technology Crime Advisory Committee is hereby established for the purpose of formulating a comprehensive written strategy for addressing high technology crime throughout the state and to advise the Office of Criminal Justice Planning on the appropriate disbursement of funds to regional task forces.

(b) This strategy shall be designed to be implemented through regional task forces. In formulating that strategy, the committee shall identify various priorities for law enforcement attention, including the following goals:

(1) To apprehend and prosecute criminal organizations, networks, and groups of individuals engaged in the following activities:

(A) Theft of computer components and other high technology products.

(B) Violations of Penal Code Sections 211, 350, 351a, 459, 496, 537e, 593d, and 593e.

(C) Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.

(D) Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.

(E) Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.

(2) To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

(3) To apprehend and prosecute individuals and groups engaged in the theft of trade secrets.

(4) To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.

(c) The Executive Director of the Office of Criminal Justice Planning shall appoint the following members to the committee:

(1) A designee of the California District Attorneys Association.

(2) A designee of the California State Sheriffs Association.

(3) A designee of the California Police Chiefs Association.

(4) A designee of the Attorney General.

(5) A designee of the California Highway Patrol.

(6) A designee of the High Tech Criminal Investigators Association.

(7) A designee of the Office of Criminal Justice Planning.

(8) A designee of the American Electronic Association to represent California computer system manufacturers.

(9) A designee of the American Electronic Association to represent California computer software producers.

(10) A designee of the California Cellular Carriers Association.

(11) A designee of the California Internet Industry Alliance.

(12) A designee of the Semiconductor Equipment and Materials International.

(13) A designee of the California Cable Television Association.

(14) A designee of the Motion Picture Association of America.

(15) A designee of either the California Telephone Association or the California Association of Long Distance Companies. This position shall rotate every other year between designees of the two associations.

(d) The Executive Director of the Office of Criminal Justice Planning shall designate the Chair of the High Technology Crime Advisory Committee from the appointed members.

(e) The advisory committee shall not be required to meet more than 12 times per year. The advisory committee may create subcommittees of its own membership, and each subcommittee shall meet as often as the subcommittee members find necessary. It is the intent of the Legislature that all advisory committee members shall actively participate in all advisory committee deliberations required by this chapter.

Any member who, without advance notice to the executive director and without designating an alternative representative, misses three scheduled meetings in any calendar year for any reason other than severe temporary illness or injury (as determined by the Executive Director of the Office of Criminal Justice Planning) shall automatically be removed from the advisory committee.
If a member wishes to send an alternative representative in his or her place, advance written notification of this substitution shall be presented to the executive director. This notification shall be required for each meeting the appointed member elects not to attend.
Members of the advisory committee shall receive no compensation for their services, but shall be reimbursed for travel and per diem expenses incurred as a result of attending meetings sponsored by the Office of Criminal Justice Planning under this chapter.

(f) The executive director, in consultation with the High Technology Crime Advisory Committee, shall develop specific guidelines and administrative procedures for the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program, which guidelines shall include the following selection criteria:

(1) Each regional task force that seeks funds shall submit a written application to the committee setting forth in detail the proposed use of the funds.

(2) In order to qualify for the receipt of funds, each proposed regional task force submitting an application shall provide written evidence that the agency meets either of the following conditions:

(A) The regional task force devoted to the investigation and prosecution of high technology-related crimes is comprised of local law enforcement and prosecutors, and has been in existence for at least one year prior to the application date.

(B) At least one member of the task force has at least three years of experience in investigating or prosecuting cases of suspected high technology crime.

(3) In order to qualify for funds, a regional task force shall be comprised of local law enforcement and prosecutors from at least two counties. At the time of funding, the proposed task force shall also have at least one investigator assigned to it from a state law enforcement agency. Each task force shall be directed by a local steering committee composed of representatives of participating agencies and members of the local high technology industry.

(4) Additional criteria that shall be considered by the advisory committee in awarding grant funds shall include, but not be limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, or corporations, as a result of the high technology crime cases filed, and those under active investigation by that task force.

(5) Each regional task force that has been awarded funds authorized under the High Technology Theft Apprehension and Prosecution Program during the previous grant-funding cycle, upon reapplication for funds to the committee in each successive year, shall be required to submit a detailed accounting of funds received and expended in the prior year in addition to any information required by this section. The accounting shall include all of the following information:

(A) The amount of funds received and expended.

(B) The use to which those funds were put, including payment of salaries and expenses, purchase of equipment and supplies, and other expenditures by type.

(C) The number of filed complaints, investigations, arrests, and convictions that resulted from the expenditure of the funds.

(g) The committee shall annually review the effectiveness of the regional task forces created in deterring, investigating, and prosecuting high technology crimes and provide its findings in a report to the Legislature and the Governor. This report shall be based on information provided by the regional task forces in an annual report to the committee which shall detail the following:

(1) Facts based upon, but not limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The number of convictions obtained in the prior year.

(E) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

(2) An accounting of funds received and expended in the prior year, which shall include all of the following:
(A) The amount of funds received and expended.

(B) The uses to which those funds were put, including payment of salaries and expenses, purchase of supplies, and other expenditures of funds.
(C) Any other relevant information requested.

SEC. 6. This act is an urgency statute necessary for the immediate preservation of the public peace, health, or safety within the meaning of Article IV of the Constitution and shall go into immediate effect. The facts constituting the necessity are:

In order to revise provisions relating to the High Technology Crime Advisory Committee and the funding of regional law enforcement high-tech task forces, so as to assist in the prevention, investigation, and prosecution of high technology crimes at the earliest possible time, it is necessary that this act take effect immediately.

Appendix A: Organizations Interviewed

AirTouch Communications	Alameda County Prosecutors Office
American Electronics Association (AEA)	American Society of Industrial Security (ASIS)
Business Software Alliance	CA Senator Pactrick Johnston Staff, 5th District
California Association of Long Distance Companies	California Attorney General's Office
California Cable Television Association	California Cellular Carriers Association
California Computer Software Producers	California Computer System Manufacturers
California Department of Justice	California District Attorneys Association
California Highway Patrol	California Internet Industry Alliance
California Office of Criminal Justice Planning	California Police Chiefs Association
California State Sherrif's Association	California Telephone Association
Comcast, Inc.	Computer Security Institute
County of Los Angeles Office of Auditor-Controller	County of Santa Clara District Attorneys Office
El Segundo Police Department	Etec Systems, Inc.
Federal Bureau of Investigation	High Tech Criminal Investigators Association
International Association of Financial Crime Investigators	International Electronics Security Group
LA - Orange Counties High Tech Crime Task Force	Los Angeles County District Attorney's Office
Los Angeles County Sheriff's Department	Microsoft Corporation, Inc.
Motion Picture Association of America	NASA Office of the Inspector General
National Law Enforcement & Corrections Technology Center-Western Region	Netscape Communications Corporation
Pacific Bell	Rand Corporation
Record Industry Association of America	Sacramento County Sheriff's Department
Sacramento High Tech Crime Task Force	San Bernardino County Sheriff's Department
San Diego Co. District Attorney's Office	San Diego High Tech Crime Task Force (being estblished)
San Jose Police Department	Search: The National Consortium for Justice and Statistics
Semiconductor Equipment and Materials International	Silicon Valley High Tech Task Force-REACT
Software Publishers Alliance	SRI, Inc.
Sun Microsystems, Inc.	U.S. Department of Commerce
University of California, Davis	US Department of Justice